DOCTORAL THESIS

Aligning IT Initiatives with Emergency Management Objectives

Vogt, Marcus

Award date:
2012

Thesis submitted in total fulfilment of the requirements of the degree of Doctor of Philosophy

Aligning IT Initiatives with Emergency Management Objectives

Developing and Adapting IT Governance Approaches for the Domain of Emergency Management

Marcus W. Vogt

Dipl. Wirt.-Inf. (DH), B. A. (Hons), M.IT (Hons)

SID: 12972939 / BUHREC: RO1026

Degree Program: PhD in Information Technology (IT 33020)

Date of Submission: 07. June 2012

Bond University

Faculty of Business, School of IT

University Drive, Robina QLD 4229, Australia

http://www.bond.edu.au

Abstract

Today's society is exposed to numerous disasters and large-scale emergencies. Information Technology (IT) can help to prevent and mitigate the effects of threatening situations if applied appropriately. However, organizations in the domain of Emergency Management feel overwhelmed by the complexity of IT. They are often unable to estimate the value and risk involved in information system and associated technologies. Thus, they are either reluctant to utilize IT, or they use inappropriate solutions. As a result, IT and Emergency Management processes are misaligned.

This thesis is investigating the benefits of strategic IT alignment in the domain of Emergency Management in order to foster the utilization of IT and realize value from it. The research has identified current IT alignment barriers and the special requirements of this domain. Emergency management has in contrast to industry to deal with unpredictable situations, multi organizational collaborations, and fast changing responsibilities and processes. Thus, this paper proposes conceptual models and methods, based on contemporary IT Governance frameworks and tools, which will help Emergency Management organizations to align IT initiatives with Emergency Management objectives.

The researcher utilized qualitative, quantitative, and modelling techniques during the different research stages in order to develop and adapt IT Governance related models and methods. The three final concepts address the most important IT Governance issues of the researched Emergency Management organizations.

"ITICO4EM", is a simplified IT Governance framework based on COBIT and ITIL. It addresses the domains needs without creating too much overhead, while it used domain specific terminology and remains ITIL and COBIT compatible.

"IT-ORG/CrIO", proposes an organizational structure for effective IT Governance in the domain of Emergency Management. It addresses the inter-organizational relations and shifting responsibilities in this domain and suggests the implementation of a mutual IT Governance approach across departments,

units, and organizations by utilizing IT Governance committees and the implementation of a Crisis Information Officer (CrIO).

“IVEM²”, will support Emergency Management organizations to estimate the value of their IT initiatives for their Emergency Management operations. The proposed IT value estimation method is based on a modular approach, which enables Emergency Management organizations to create an IT portfolio, which can cope with uncertain emergencies and deliver value in all possible situations.

Finally, the three approaches are combined to the “ITEM-Governance Approach”, which should support Emergency Management organizations in their endeavour to align their IT initiatives with Emergency Management objectives in order to increase IT value, reliability, and utilization.

Acknowledgements

This thesis is dedicated to all families who lost a loved one during large scale emergencies and disasters.

First, I would like to thank my supervisors **Prof Dr Gavin Finnie,** who supported my PhD application and enabled me to commence my research, **Prof Dr Kieth Hales,** who guided my studies in Australia, and **Prof Dr Dieter Hertweck,** who unselfishly agreed to supervise me in Germany. Their support, comments, suggestions, and constructive criticism helped me to develop my skills and enabled me to finish this research project successfully. I would also like to thank the rest of the **faculty and all other PhD students** for all the interesting and fun conversations during a coffee break; your input helped me to see my research from a different angle.

Additionally, I would like to thank **all participating organizations, interviewees, and participants,** who helped me to collect the data and discussed my intermediate and final results. This thesis would not have been possible without their help and trust. I hope the participating organizations will find this thesis helpful to improve their emergency services even more. Their dedication to help others has been an inspiring example to me.

Finally, I want to thank **my family and friends,** who always supported and encouraged me during my time as a PhD student. Special thanks go to my wife, who had to renounce a lot during the past three years, my dad, who has always been my role-model and taught me to stand tall even in hard times, my mother who had never the chance to see me growing up but gave me guidance from above, and last but not least my grandmother for all her prayers and love.

Thank you all

Statement of Originality

This thesis is submitted to Bond University in fulfilment of the requirements of the degree of Doctor of Philosophy. This thesis represents my own original work towards this research degree and contains no material which has been previously submitted for a degree or diploma at this University or any other institution, except where due acknowledgement is made.

Marcus W. Vogt

Baden-Baden, Germany 07/06/2012

Author's Publications

Vogt, M. (2009) *"ICT Governance & Disaster Management"*, PhD Curriculum Proceedings of the 6th International ISCRAM Conference, Gothenburg, Sweden

Vogt, M., Hales, K. (2010) "*Strategic Alignment of ICT Projects with Community Values in Local Government*", Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS 2010), Hawaii, USA

Vogt, M., Hales, K., Hertweck, D., Finnie, G. (2010) "*Strategic ICT Alignment in Emergency Management"*, Proceedings of the 7th International ISCRAM Conference, Seattle, USA

Vogt, M., Hertweck, D., Hales, K. (2011) *"Strategic Alignment in Uncertain environments: An Empirical Study in Emergency Management Organizations"*, Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2011), Hawaii, USA

Vogt, M., Hales, K., Hertweck, D. (2011) "*Optimizing IT portfolios in Emergency Management Organizations - A modular alignment approach*", Proceedings of the 8th International ISCRAM Conference, Lisbon, Portugal

Vogt, M., Küller, P., Hertweck, D., Kieth, H. (2011) "*Adapting IT Service Management Frameworks Towards Domain Specific Requirements: An Empirical Study in the Domains of Small & Medium Enterprises (SME) and Emergency Management (EM)*", Proceedings of the 17th Americas Conference on Information Systems (AMCIS 2011), Detroit, USA

Küller, P., Vogt, M., Hertweck, D., Grabowski, M. (2011) *"A Domain Specific IT Service Management Approach for Small & Medium Enterprises"*, Proceedings of the 16th International Business Information Management Conference (IBIMA 2011), Kuala Lumpur, Malaysia

ACCEPTED BUT NOT YET PUBLISHED:

Vogt, M., Hales, K. (2012) "Alignment of IT Projects and Investments to Community Values", in "From Government to E-Governance", Edts. M. M. Islam & M. Ehsan, IGI Global, Hershey, Pennsylvania, USA

Vogt, M., Küller, P., Hertweck, D. (2012) "*Adapting IT Governance and ITSM Methods: A Domain Specific Approach*" in "Corporate Governance and Enterprise Systems: Technological Solutions", Edts. T. Lazarides & M. Argyropoulou, IGI Global, Hershey, Pennsylvania, USA

Küller, P., Vogt, M., Hertweck, D., Grabowski, M. (2012) "*IT Service Management Approach for Small & Medium-Sized Enterprises. A Domain Specific Approach* ", Journal of Innovation Management in Small and Medium Enterprises, IBIMA Publishing, USA

Contents

List of Figures

List of Tables

Abbreviations

AUS	Australia
BVIT	Business Value of Information Technology
BSI	(1) British Standards Institution
	(2) Bundesamt für Sicherheit in der Informationstechnik
	(German Federal Office for Information Security)
CIMS	Critical Incident Management Systems
CM	Crisis Management
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and related Technology
CRED	Centre for Research on the Epidemiology of Disasters
DM	Desaster Management
DRF	Deutscher Rettungsflug (Flight Rescue Germany)
DRK	Deutsches Rotes Kreuz (German Red Cross)
EM	Emergency Management
EMQ	Emergency Management Queensland
FEMA	Federal Emergency Management Agency
GER	Germany
GIS	Geo Information Systems
GPS	Global Positioning Systems
HPITSM	Hewlett Packard's ITSM Reference Model
IAEM	International Association of Emergency Managers
IFRC&RDS	International Federation of Red Cross & Red Crescent Societies
ICT	Information and Communication Technology

IS	Information Systems
ISO	International Organizations for Standardization
ISCRAM	Information Systems in Crisis Response and Management
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
ITGI	IT Governance Institute
IT-GOV	IT Governance
MOF	Microsoft Operations Framework
NGO	Non-Governmental Organization
NPV	Net Present Value
NICTA	National ICT Australia
NRC	National Research Council
PMBOK	Project Management Book of Knowledge
PRM-IT	Process Reference Model for IT
RISK IT	Risk of Information Technology
ROI	Return of Investment
SARS	Severe Acute Respiratory Syndrome
VAL IT	Value of Information Technology

PART I:

Introduction & Theoretical Background

1 Introduction, Motivation & Research Problem

Due to globalization, intercontinental flights, industrialization, and an increasing demand for energy, which is suspected to be the cause of global warming, today's society is exposed to numerous threats:

- Permanent risk of global terrorism (e.g.: New York 2001, Bali 2003/2005, Madrid 2004 and London 2005/2007)
- The persisting threat of pandemic diseases (e.g.: SARS 2002, bird-flu 2005/2006, and swine-flu 2009)
- An increasing number of natural disasters (e.g.: Tsunami in the Indian Ocean 2004, Hurricane Katrina in New Orleans 2005, , earthquake in Sichuan-China 2008, Cyclone Nargis in Myanmar/Burma 2008, earthquake Haiti 2010) and of course recurring hazards from bushfires, wildfires, droughts, heat waves or severe floodings (e.g. in Australia 2009, California 2007/2008 and Germany/Austria 2009)
- Industrial accidents ('Fireworks Disaster' in Enschede-Netherlands 2000), large scale accidents ('Train Disaster' in Eschede-Germany 1998)
- Nuclear accidents or incidents (e.g.: Meltdown in Chernobyl in 1986 and Fokushima 2011)

Protecting the population from the aftermath of natural disasters and man-made threats requires extraordinary attention from authorities and non-governmental organizations (NGOs).

Well-functioning infrastructures are vital in today's high-tech society and economy. We are highly dependent on secure and consistent water and energy supplies as well as reliable Information Technology (IT). Major failures of these important infrastructures, caused accidentally, by intent or by an act of nature beyond control can result in serious consequences for the population and environment (Barton, 2007; Borodzicz, 2005).

Communication and information play an essential role during the different stages of an emergency or crisis situation. Accurate information at the right time and at the right place can save lives. Today, IT can significantly increase information richness and reach (Iannella & Henricksen, 2007). However, to be

useful the applied technology has to be reliable, appropriate, and usable; otherwise, technology is more a hindrance than an improvement.

Literature and preliminary research results from a focus group have shown that IT Service Management (ITSM) and IT Governance (IT-GOV) methods are barely used or even unknown to decision makers within the domain of Emergency Management. However, in an extensive study by the United States FEMA (Federal Emergency Management Agency) and the National Research Council (NRC), IT has been identified as one of the most promising success factors to improve Emergency Management processes but its value and contribution is often unclear to emergency managers and involved organizations. In this study, which was conducted from 2005 to 2007, FEMA and NRC investigated the role of IT in Emergency Management and identified that IT alignment and IT value creation is most important for a successful implementation and utilization of new technologies. Nevertheless, there is lack of understanding and suitable methods to realize the benefits of IT by Emergency Management organizations and related authorities. As a result they are unable to align their processes and IT effectively (Rao, Eisenberg, & Schmitt, 2007).

The findings of the FEMA / NRC report overlap with the researcher's own findings from initial conversations with Emergency Management professionals in Germany and Australia. Similar results have also be confirmed by a related research project, which was recently conducted in Swedish municipalities by Weyns & Höst (2009). They have published results, where interviewed emergency managers and involved IT personnel confirm that IT is not properly used because decision makers in EM and IT do not work hand in hand; they "just try to solve the problems that come up…and…don't 'know what the rules are for prioritized service in an emergency" (Weyns & Höst, 2009, pp. 3,4).

In contrast to Emergency Management, commercially driven organizations utilize IT Governance methods and tools to manage information and technologies quite successfully. Clear responsibilities, optimized IT portfolios, aligned systems, transparent risks and reliable services are key factors for their success and ensure competitive advantage. Frameworks such as COBIT, ITIL, CMMI, Val-IT, ISO27000, ISO20000, and ISO 38500 provide implementation

guidelines and best practices for these companies (IT Governance Institute, 2003; Weill & Ross, 2004).

However, most of these guidelines and best practices are optimized for commercially driven organizations with rather long-term goals, stable hierarchies, and off-the-shelf products. Conversely, the domain of Emergency Management demands different approaches because each emergency or disaster is unique, so most countermeasures and teams will differ from case to case. Therefore, information channels and the information requirements change according to the scenario. Moreover, decision rights and responsibilities shift during the transition from day-to-day business to emergency processes. Hence, most emergency managers demand solutions that are flexible and reliable, but in their view existing IT Management frameworks are too complex or have too rigid processes. Thus, they cannot be applied without adaptation (Rao, et al., 2007; Weyns & Höst, 2009).

It is a common understanding that improving Emergency Management processes is crucial in order to save lives and preserve the community and environment. IT has the potential to improve such processes and support emergency managers and first responders in their routines. However, research in this area is in an early stage and reusable data is hard to find. Since there is not enough preliminary research done in this particular area, almost all data had to be collected by the researcher himself. To get a diverse view on the topic various sources of information have been used: interviews, surveys, case studies, and modelling techniques.

The primary objective of this research was to develop conceptual models and methods (cp. Frank, 1999) that enable Emergency Management organizations to realize value and benefits from their IT initiatives and therefore utilize these technologies and services more effectively and efficiently. Thus, the researcher investigated how IT and Emergency Management can be aligned and managed in order to improve emergency preparation and response. Therefore, the challenge of this research was to develop new models and methods, based on existing frameworks, which are able to cope with the unpredictable nature of disasters and crises, and improve the overall IT-Governance and strategic IT alignment of Emergency Management organizations. The developed models

and methods were tailored towards these organizations' needs and address their problems on a socio-technical level by improving IT Governance and IT Service Management processes, organizational structures, and IT value estimation methods.

To achieve these objectives different research steps were necessary which are described in six consecutive sections.

Part I will introduce the reader to the topic and discusses the theoretical background. Objective of this section is to highlight the research gap in the existing literature

Part II will discuss the research structure and design. Aim of this section is to describe the research questions in more detail and discuss appropriate research methods.

Part III will describe the data collection and analysis methods chosen. Objective of this section is to show the reader how data was collected and how conclusions were drawn from interviews, observations, and cases studies.

Consequently, Part IV discusses the conceptual models and methods developed from the previously drawn conclusions. The goal of this section is to provide the target group (Emergency Management Organizations) new models and methods to improve their IT Governance performance and increase their strategic IT alignment in order to create value from their IT investments.

Part V summarizes the findings and gives recommendations for future research.

Part VI provides the reader with an extensive appendix including more detailed information about the developed models and methods, as well as collected data and literature resources used.

In detail, the thesis is structured as follows:

After a brief introduction in the current chapter, chapter 2 will give the reader an overview of the existing research on the topic. Thus the author conducted a thorough literature review in the areas of Emergency Management (Chapter 2.1), IT Governance and Strategic IT Alignment (Chapter 2.2), and IT / IS and its Management in the Domain of Emergency Management (Chapter 2.3),

which eventually enabled the author to identify the research gap and to form the research questions.

Consequently, Chapter 3 elaborates this research gap and the thesis' contribution to the domain.

Chapter 4 explains the research design. It discusses the underlying epistemological foundation (Chapter 4.1) and the applied research methods (Chapter 4.2) so the reader can follow the author's research steps in the coming chapters.

In chapter 5 the thesis discusses different data collection methods and information resources in order to explain to the reader from whom and how the data was derived and on what basis the author has built his conclusions.

Chapter 6 describes the data analysis process of the interviews (Chapter 6.1) and the cases studies (Chapter 6.2). This chapter explains in detail how the author has analysed each information resource and gives vivid examples of problems in this area.

Consequently, the results from each information resource are discussed and combined in chapter 7 and chapter 8 to draw generalized conclusions from the data which are the foundation for the conceptual IT Governance models for the domain of Emergency Management.

In Chapter 9 the author explains the conceptual models and methods developed based on the findings from previous chapters. The chapter describes an integrated solution (Chapter 9.4) for the three core IT Governance issues of the EM domain: ITICO4EM (Chapter 9.1), IT-ORG /CrIO (Chapter 9.2), and IVEM² (Chapter 9.3). The developed models and methods should provide other organizations in this domain a guideline to improve their Strategic IT Alignment and their overall IT Governance performance.

Finally, chapter 10 evaluates the conceptual models and methods by means of expert judgements and a representative application of the developed methods in one of the case studies.

The thesis closes with a final conclusion (Chapter 11) and recommendations for future research (Chapter 12), followed by the appendix and bibliography.

2 Theoretical Background and Existing Research

The following literature review is split into four sections. The first part will roughly describe the domain of Emergency Management including relevant definitions. The second part will explain the different methods and frameworks in the area of IT Governance and IT Service Management. The third part will describe the current IT situation in the domain of Emergency Management. It will illustrate what has been done in this research area, including existing problems, presumed potentials of IT, and promising technologies. The fourth part will summarize the findings and highlight the identified research gap.

2.1 Emergency Management

Emergency Management (EM) plays a vital role in today's society. For centuries, humanity has faced disasters and large-scale emergencies of all kinds. During that time, they developed countermeasures and procedures to avoid or mitigate the impact of natural or manmade disasters based on their experience and technological progress. The collected knowledge is the foundation of today's EM. However, the likelihood and impact of different disaster/emergency situations, as well as the corresponding countermeasures, have changed over time and will continue to do so. Therefore, the discipline of EM has to be continuously adapted and improved.

2.1.1 Definition of Crisis, Disaster, and Emergency

The literature review has shown that there is no single shared definition for crisis, disaster, or emergency per se. Many attempts have been made to define what a disaster or emergency is, but all are either too general or too specific to cover all purposes. However, most definitions share one thing in common: They imply the need for external assistance of supporting organizations or authorities to master threatening situations. Since most of the definitions overlap in their core, this research will use the terms crisis, disaster, and emergency interchangeably (Brennan & Krohmer, 2005; Shaluf, Ahmadun, & Mustapha,

2003). Nevertheless, to maintain clarity a working definition is used based on two widely known definitions.

The following definition is used by the Centre for Research on the Epidemiology of Disasters (CRED) in Brussels, Belgium:

“A disaster is a situation or event which overwhelms local capacity, necessitating a request to a national or international level for external assistance” (Brennan & Krohmer, 2005, p. 201).

Another definition is used by the Red Cross Federation in Geneva, Switzerland:

“Disasters are exceptional events which suddenly kill or injure large number of people or cause major economic loss” (IFRC&RCS, 1998, p. 12).

As a result, the following working definition of for crisis, disaster, or emergency is used:

“A crisis, disaster, or large scale emergency in the broadest sense is a situation which is threatening a large number of people or important economic and ecological infrastructures and requires assistance of national or international organizations and / or authorities to minimize or prevent its impact”

2.1.2 Definition of Crisis-, Disaster-, and Emergency Management

Since the definition of a crisis, disaster, or emergency can be ambiguous, the definition of crisis management, disaster management, or Emergency Management can have different facets or meanings as well, but also share a common denominator. Similar to the terminology above, crisis-, disaster-, and Emergency Management are often used as synonyms. Nonetheless, a working definition is used to avoid too much ambiguity about its scope.

Foundation for the working definition is the definition of Queensland’s Disaster Management Act 2003:

“Disaster management means arrangements about managing the potential adverse effects of an event, including, for example, arrangements for mitigating, preventing, preparing for, responding to and recovering from a disaster” (Emergency Management Queensland (EMQ), 2009, p. 14).

Secondary the definition of the International Association of Emergency Managers (IAEM) is used as a source for the working definition of disaster or Emergency Management:

“Emergency management is the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters” (IAEM, 2009, p. 1).

Combining the two definitions above the following working definition is used:

“Crisis -, Disaster-, or Emergency Management is the managerial function which arranges countermeasures and coordinates involved organizations and/or units to prevent, mitigate, respond to, recover from or prepare for a disaster and therefore reduce the overall vulnerability of communities and infrastructures to known and unknown threats”

2.1.3 Different Phases in Emergency Management

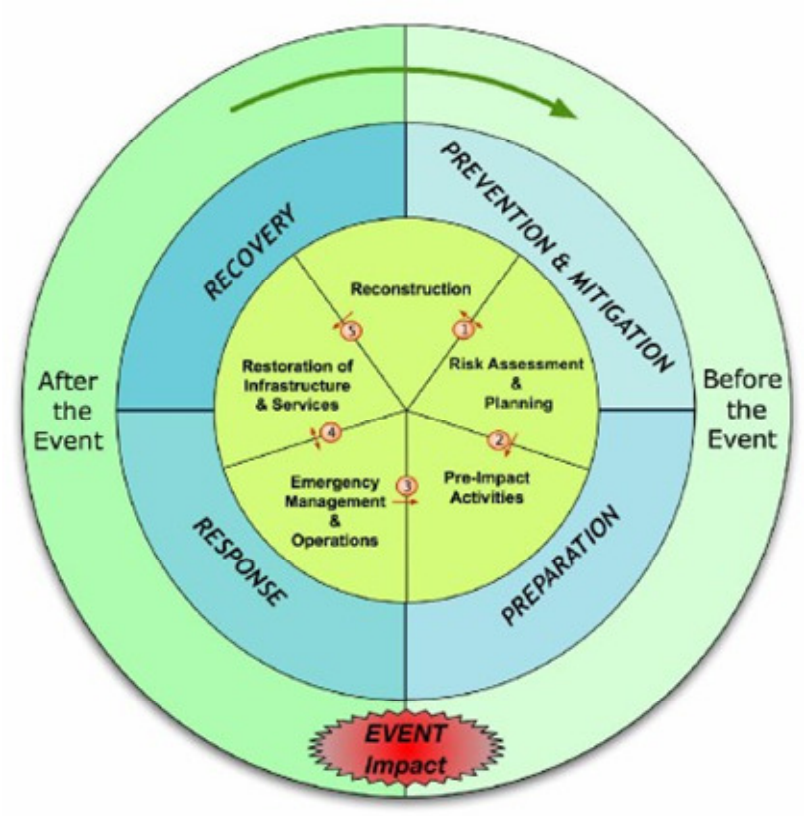


Figure 1: Emergency Phases (FLOODsite & SOGREAH, 2009)

Emergencies can be categorized in different ways. In this research, emergency situations are divided into four phases according to IAEM (2009): Prevention & Mitigation, Preparation, Response, and Recovery / Relief, as shown in Figure 1.

2.1.3.1 Prevention & Mitigation

Preventing a disaster or its consequences should be the prime directive for every organization or administration involved in Emergency Management procedures. Early warning, forecasting, and monitoring systems have been improved significantly over the past 10 years. New technologies and methods have enabled such a progress. The utmost crucial factor in disaster prevention is time. The earlier an upcoming threat is known the better people and organizations can apply countermeasures to prevent a hazardous outcome. This means that all involved EM organizations and authorities must plan ahead to identify preventative and protective measures before a disaster strikes (Turoff et al., 2009; Wisner & Adams, 2003).

2.1.3.2 Preparation

If a disaster cannot be prevented, being prepared for it is the second most important phase. Unfortunately, one cannot be prepared for every kind of emergency. Even if a disaster is of the same kind (e.g. flooding) its severity, extent, and progress cannot be rehearsed in every facet. The situation, however, can be compared to a football game. Each game for itself is unique; though, endurance, strength, fitness, health and the knowledge of different tactics can influence the outcome of a game significantly. The same principle can be applied in Emergency Management. Preparing for the unknown by providing reliable equipment and tools, having a good organization, educating the team, and having a repertoire of best practices can be crucial in hazardous situations. Nevertheless, it is essential that all levels of government and volunteers undertake a thorough vulnerability analysis, which assesses the variety in types, impact, and frequency to formulate possible regulations and emergency plans (Turoff, et al., 2009; Wisner & Adams, 2003).

2.1.3.3 Response

In case of an unforeseen disaster the response teams and emergency managers have to act as fast as possible to prevent additional damage. Preparation can help to mitigate the consequences in first place but ad-hoc decisions are needed to react to such a threat and moderate its impact. Fast decision-making is the key for success. The faster and more precise a decision can be made on a strategic level the faster the operational teams can react (Turoff, et al., 2009). To make the right decision two things are most crucial. First, the right information at the right place and in the right time (Iannella & Henricksen, 2007). Every decision can only be as good as the information on which it is based on; otherwise, it might only be a good or bad guess. Second, fast communication and information flow between operational and strategic levels is crucial. In a case of an emergency a situation can change within seconds and, thus, communication and information flow has to be fast and reliable (Wisner & Adams, 2003).

2.1.3.4 Recovery / Relief

Sometimes a disaster can happen within seconds or minutes and cannot be prevented or mitigated (e.g. earthquake) but its affects can be seen for years and people suffer under the long-term consequences (e.g. Haiti 2010). Efficient disaster relief can help them to get back their normal life. Food, water, medical supplies, and shelter are the most vital ones. Additionally, important infrastructures have to be back as fast as possible to ensure the provision of goods, services and information. Proper logistics, infrastructure maintenance, and supply management are therefore crucial means in disaster relief (Wisner & Adams, 2003).

2.1.3.5 Different Forms of Crisis Progress

There are not only different phases during a disaster or large-scale emergency, also the time line of a disaster is crucial to its response. Some disasters strike out of sudden, others have recurring patterns or follow a waveform, and a few have a creeping time-line. As a result, EM organisations and authorities have

difficulties to prepare for all these different types. Particularly the very short termed events are problematic since they are hard to predict and therefore preparation is not very precise (Guha-Sapir & Lechat, 1986). Figure 2 gives an example of these different patterns (Bundesministerium des Inneren, 2008, p. 10).

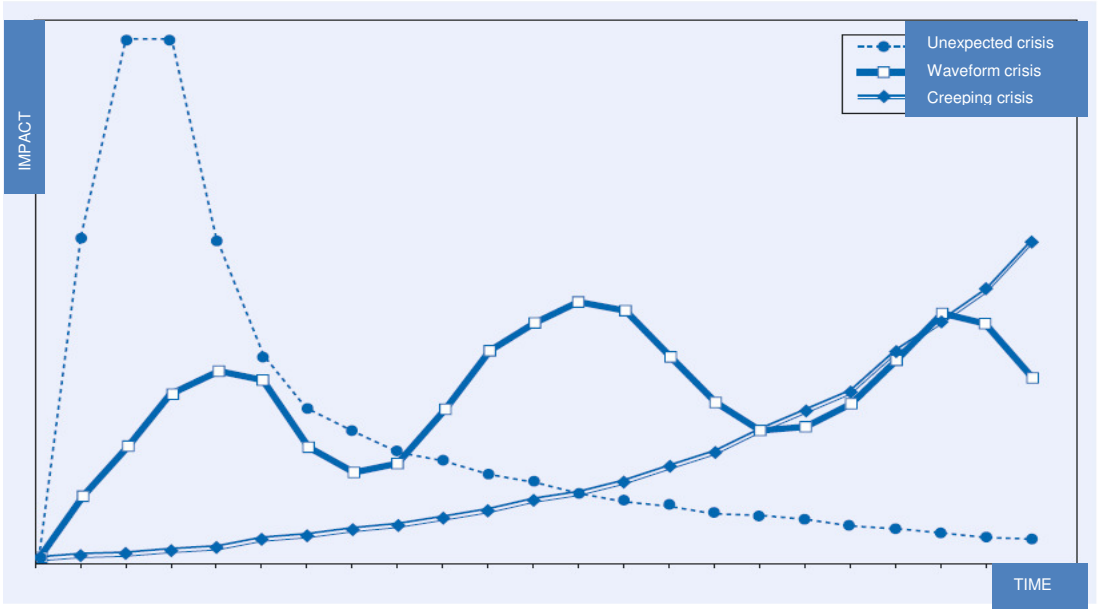


Figure 2: Crisis Progress

Examples for these different forms are:

- Unexpected Crisis: Either this could be a natural disaster such as an earthquake or Tsunami, or it could also be a man-made disaster such as a nuclear fallout or terror attack. Just recently in 2011, we could witness the destructive force of a combination of the natural and manmade disasters in Japan where an earthquake resulted in a big Tsunami, which, in turn, destroyed important infrastructure of several nuclear plants. As a result, the destruction and operational mistakes led to a severe nuclear fall-out.
- Waveform Crisis: A waveform crisis is usually the cause of social, political, or economic problems. In relation to this thesis, this could be for example riots or rebellions as seen in 2011 in several Arabic countries. Nevertheless, there are also some natural phenomena such as bushfires or droughts. A waveform crisis can be predicted to a certain extent e.g.

there is a higher likelihood of bushfires during a particular time of the year, but they can take unforseen turns, in terms of severity and impact.

- Creeping Crisis: The impact and effects of a creeping crisis or disaster can usually be predicted and foreseen. Hence, counter measures can be planned in relative detail in order to mitigate the effects. One example of a creeping crisis could be a pandemic. In 2009/2010 we have seen the effects of the swine flu worldwide. However, due to its creeping character the authorities were able to react to this threat and a full-blown pandemic was prevented.

With regard to information management and IT-Management, all three variations have their difficulties. Even though most EM organizations and authorities try to use relative realistic emergency situations as a basis for their responses and emergency drills, they cannot cover all possibilities. This is particularly true for unexpected large-scale emergencies or disasters. The question in case of such a situation is: Which processes and technologies do we need to mitigate the actual situation (Rao, et al., 2007; Turoff, 2002; Van de Walle & Turoff, 2008).

Training scenarios for most waveform and recurring emergencies are usually much more detailed and realistic. Countries or states, which are frequently struck by bushfires or floods, have experience with these kinds of emergencies. Hence, their countermeasures are usually quite effective. Nevertheless, this also bears some problems. When an emergency situation becomes bigger than usual or takes unexpected turns, authorities and EM organizations struggle to master the situation. Particular inter-organizational / cross-border communication and information flow as well as an effective utilization of shared resources and logistics becomes critical in these situations (Chaczko & Ahmad, 2005; Palen et al., 2010).

In contrast to previous pandemics such as the Great Plague / Black Death / Cholera between the 14th and 19th century, or the Spanish flu in 1918, the latest pandemics such as SARS (2002/2003), bird flu/H5N1 (2006/2007) and swine flu/H1N1(2009/2010) did not have such a severe impact. This is not only the result of an improved medical system but also because of an improved information flow between countries, states, municipalities, authorities, EM

organizations, and critical infrastructure providers (Bandayrel, Lapinsky, & Christian, 2011; Brownstein et al., 2010).

As one can see, information and technology management are crucial for most EM organizations and authorities in order to respond to large-scale emergencies or disasters. The effective and efficient utilization of information and technology is, or should be, an important issue to decision makers within these organizations. Moreover, the developers of EM related IT systems and management methods should keep in mind the dynamics of this domain and address them accordingly (Turoff, Chumer, Van de Walle, & Yao, 2004).

2.2 IT Governance and Strategic IT Alignment

According to Luftman and Kempaiha (2007) IT Governance and its related frameworks and methods are seen as an enabler to achieve strategic IT alignment. Its goal is to enable the transition from a strategic to an operational level without losing the focus on business objectives. Thus, as shown in Figure 3, IT Governance and IT Service Management can bridge the gap between Corporate Governance and operational IT Management and enables them to achieve strategic IT alignment, whereas the IT strategy is made on board level and IT Management is focusing on technological transition (Böttcher, 2008).

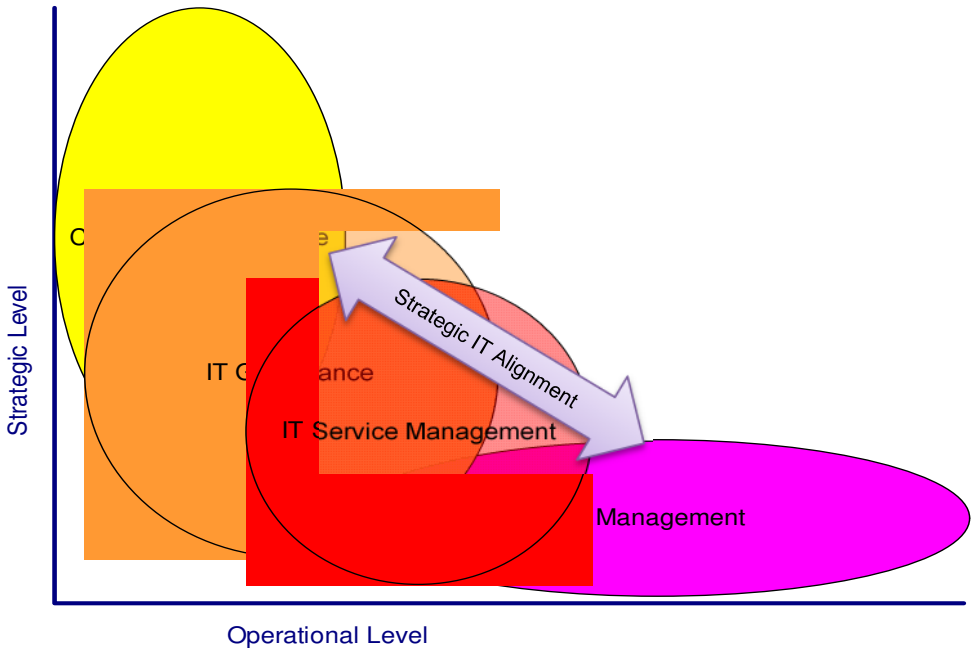


Figure 3: IT Governance in relation to other approaches

2.2.1 IT Governance

IT Governance has inherited much from Corporate Governance and IT Management. However, since there are overlaps between the three disciplines, its definition became ambiguous and resulted in various descriptions, which can be found in literature (Simonsson & Johnson, 2006). The most common ones are:

"IT Governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives" (IT Governance Institute, 2003, p. 10).

"IT Governance is the organisational capacity exercised by the Board, executive management and IT Management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" (Van Grembergen, 2002, p. 7).

"IT Governance: Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT" (Weill & Ross, 2004, p. 8).

However, these definitions are mainly applied to commercially driven organizations and have to be adapted to fit into the domain of Emergency Management. Hence, a working definition has been created, which will be used throughout this paper:

"IT Governance, with respect to the domain of Emergency Management, is the responsibility of politicians, public representatives, executive managers, emergency managers, and IT personnel of these organisations. It is an integrated part of their responsibility towards the society and political directives to ensure the reasonable, effective, and efficient use of IT to support preparations and actions to mitigate and avoid the impact of disastrous situations."

According to Van Grembergen, De Haes, & Guldentrops (2003, p. 18) there are *"two important elements of IT Governance: value delivery (which is the goal) and strategic alignment (which is the means)."* The ITGI (2003) adds a third element "Risk Management" and a fourth element "Performance

Measurement". All parts are equally important to balance opportunities and threats when a decision for an IT project or investment is made. Within the context of Emergency Management well-functioning and suitable IT systems cannot only save money, they can also save hundreds of lives. Therefore, it is more than appropriate that IT is strictly aligned with their strategic goals. In our case, the strategic goal is to mitigate and avoid catastrophic impacts of different emergency situations as effectively and efficiently as possible. The value of an IT system can therefore not be expressed in Dollars or Euros; the value of IT is derived from how well it supports Emergency Management groups and processes. Risk and performance measurement can be applied to assess the reliability of IT systems and IT services. Therefore, properly managed risks and opportunities can increase trust in and value of IT enabled Emergency Management processes.

Van Grembergen et al. (2003) stress that these definitions have one major thing in common: The link between business and IT; so called "alignment". All governmental and non-governmental organizations have one common strategic goal in the event of an emergency: Saving lives and protecting critical infrastructures. However, since this is a rather general strategic goal and the majority of disasters are highly unpredictable, achieving a high level of strategic IT alignment remains a challenge to NGO's and authorities.

2.2.1.1 Strategic Alignment

As stated above, the link between IT and the business is the crucial factor in IT Governance (Van Grembergen, et al., 2003). Moreover, the coexistence between IT functions and non-IT functions within an organization is not enough, they have to be joined together to gain leverages and achieve the strategic goals (Duffy, 2002).

Henderson's and Venkatraman's (1992) Strategic Alignment Model (SAM) (see Figure 4) is based on four main areas of strategic alignment (squares), which consist of three underlying components (ovals) that influence each area. The squares are separated vertically in internal and external views and horizontally in IT and business perspectives. Between those quadrants, they firstly identified the need for a strategic fit (vertical), which defines how well operations fit to

strategic direction of the IT or business perspective. Second, they identified a functional integration (horizontal) between IT and business on strategic and operational levels. Even though all areas affect each other, the horizontal relationship has been identified as the most crucial factor for the alignment of business and IT.

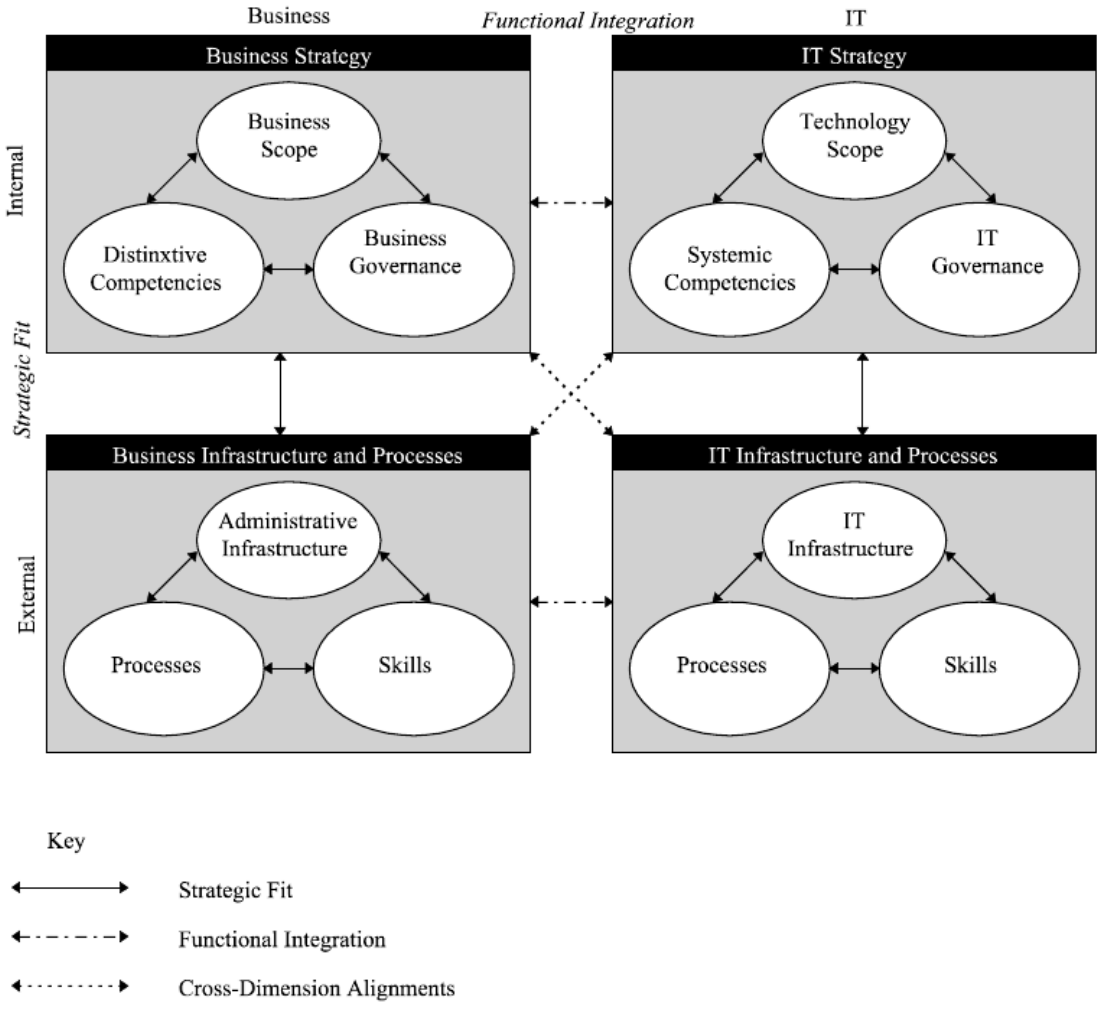


Figure 4: Strategic alignment model (Henderson & Venkatraman, 1992)

However, as with IT Governance there is no single definition in the literature for "Strategic IT Alignment". Different researchers have used synonyms for their definitions. For example:

- "Integration" is used by Weil & Broadbent (1998)
- "Fusion" is used by Smarczny (2001)
- "Symbiosis" is used by Duffy (2002)
- "Harmony" is used by Luftman (2003)

According to Chan (2002, p. 111) alignment is not a static status. It is rather a consistently developed process. “The ‘bringing in line’ of the IS function’s strategy, structure, technology and processes with those of the business unit so that IS personnel and their business partners are working towards the same goals while using their respective competencies.”

All of these definitions aim at the integration of IT and business strategies. In this research project, an adapted definition by Duffy (2002) will be used. Strategic Alignment is “… the process and goal of achieving competitive advantage through developing and sustaining a symbiotic relationship between business and IT” (in Van Grembergen, et al., 2003, p. 7).

In the context of Emergency Management, the term “competitive advantage” has to be substituted by “optimal support in an emergency or disaster” and the term “business” refers to the duties of emergency managers and related personnel. Furthermore, the terms “Strategic Alignment”, “Strategic IT Alignment”, “IT/Business Alignment” and “Alignment” are used interchangeably in this document but are always linked to this definition.

2.2.1.2 Compliance

In addition to “Alignment”, “Compliance” is another driver for IT Governance implementations in industry. Scandals as WorldCom or Enron created severe turbulences in the US financial sector and stock markets. In response new regulations and legislations, such as Sarbanes-Oxley Act (SOX), Basel II and other national rules, were developed to increase the transparency of a company’s procedures and transactions and regain the trust of investors (Chorafas, 2004; Fischer, 2002; Schwaiger & Urbina, 2006; Welch & Welch, 2005).

Even though SOX or BASEL II might not affect disaster management, the domain has to comply with other legal regulations. In particular Data Protection Acts and Privacy Acts (e.g. Directive 95/46/EC, UK Data Protection Act 1998) play an elemental role when information systems are designed for EM purposes or information between different NGOs and authorities is exchanged

before, during, or after an emergency situation (European Union (EU), 2009; Office of Public Sector Information (OPSI), 1998).

2.2.2 IT Service Management (ITSM)

IT Governance has been developed to align business goals and IT initiatives (Böttcher, 2008; Elsässer, 2005). However, the alignment of IT initiatives is not enough to realize value of an IT related investment, also the long-term maintenance of the value plays a paramount role for a successful IT strategy. IT Service Management (ITSM) is a subset of IT Governance with strong relation to operational and strategic dimensions (see Figure 3, p.35). Therefore, ITSM is an appropriate approach to assess and improve strategic IT alignment and transfer the long-term strategy into the day-to-day IT operations. Due to its strategic and operational components, ITSM should be able to support all stages of Emergency Management (prevention, preparation, response, and recovery – see Figure 1, p.30).

The most common definition of ITSM is written in the IT Infrastructure Library (ITIL) Framework and supported by the IT Service Management Forum (itSMF):

IT Service Management is concerned with the delivery and support of services that are appropriate to the business requirements of an organisation promoting a quality approach to achieving business effectiveness and efficiency in the use of information systems (Taylor, 2000). However, a more precise definition of ITSM is:

“IT Service Management is the planned and controlled utilisation of IT assets (including systems, infrastructure and tools), people and processes to support the operational needs of the business as efficiently as possible whilst ensuring that the organization has the ability to quickly and efficiently react to unplanned events, changing circumstances and new business requirements as well as continuously evaluating its processes and performance in order to identify and implement opportunities for improvement.” (Addy, 2007, p. 46).

For the purpose of this research the second definition of ITSM by Rob Addy (2007) is sufficient enough if we link the term “business” to Emergency Management.

ITIL and ISO 20000 are the best-known standards or best practices for ITSM and both are strongly related to each other. They share similar principles and methods to provide better services for the organization and even complement each other in some facets. Mutually they pursuit and focus on three premises to improve IT Service Management:

- What has to be done now?
- What has to be done if something goes wrong?
- What do we have to do to make things better?

By answering these questions, they both follow the principle of IT alignment as illustrated in the previous chapter. Addy (2007, p. 45) describes this as “aligning …assets, people, and processes to support the operational needs of the business” in order to ensure “that the service delivery function is contributing to the success of the business and helping to drive the organization forward.”

2.2.3 Existing IT Governance / ITSM Frameworks

"You can't manage what you can't measure", is an often-used quote in business management and can be applied in IT Management too. According to Porter (2008) all actions taken in an organization must add value or they are just wasting money, time and other resources. However, this leaves the question, how can we determine intangible values and risks in complex IT projects or systems? Emergency managers, fire fighters, or politicians might not understand IT terminology or see the bigger picture and benefits of an IT initiative if it is not linked to a business process. Values, opportunities, and risks must be explained in a way that can be understood by IT and business units. Particularly, non-technology savvy decision makers need to realize how IT can support and improve their efforts, but also understand what risks IT enabled processes can bear. Moreover, they have to understand that IT is not a ‘magic and unintelligible black box’ but can be a ‘reliable and useful tool’ for their daily work if managed properly. IT Governance and ITSM frameworks and methods can be a solution.

Peterson (2003) and Van Grembergen et al. (2003) suggest that IT Governance should be implemented by a framework of structures, processes, and relational mechanisms.

According to Bhattacharjya & Chang (2007, p. 3) “A number of international standards such as Control Objectives for Information and Related Technology (COBIT), ISO17799, IT Infrastructure Library (ITIL) and Capability Maturity Model (CMM), Project Management Body of Knowledge (PMBOK), are now available to IT organizations to help them improve their accountability, governance, and management.”

Frameworks such as COBIT or ITIL can help organizations to get the most out of their IT investments and align their IT services. However, such complex Frameworks cannot be implemented over night and need time to adapt to an organization’s individual needs. This is particularly difficult since the domain of Emergency Management has very unique rules and requirements due to the unpredictable nature of disasters, inter organizational collaboration and ad-hoc teambuilding. Iannella, Robinson, and Rinta-Koski (2007) argue that most models or frameworks cannot be designed in a way that all possibilities can be catered for a priori.

Catastrophes and emergencies are usually unforeseen and vary largely in their progress, impact, and severity. Thus, each situation needs an individual solution. As a consequence, rigid and commercially driven IT Governance methods are usually of lesser value to Emergency Management and first-responders. Nevertheless, these frameworks can provide some structured guidance, which can lead to an improved IT Governance maturity. Moreover, these frameworks and tools can be used conjointly to overcome their individual weaknesses (IT Governance Institute, 2008b; IT Service Management Forum, 2009a).

The following paragraphs will briefly describe the most common IT Governance and ITSM frameworks.

2.2.3.1 Calder-Moir Framework

An excellent way to combine multiple tools and frameworks together is to use an even more holistic approach. The Calder-Moir IT Governance Framework "is a straightforward tool for organising and communicating IT Governance issues and activities" (Calder & Moir, 2009, p. 1). Calder's and Moir's method does not provide a new solution; it is rather a joint collection of existing frameworks as ITIL, COBIT and ISO 27000. It organizes these tools and methodologies to support all organizational hierarchies, the board, executives, and practitioners, and places them in an end-to-end context. This provides a simple reference point to discuss all facets of IT direction and performance. The framework is built upon six segments and each of them symbolizes one step in the end-to-end process that starts with business.

As one can see in Figure 5, the framework covers all aspects of IT Governance including but not limited to technology management, risk management, strategy, intellectual property, business design, project management, and compliance (Calder & Moir 2006). The following frameworks, which seem to be most relevant for the ongoing research, are all part of this holistic approach.

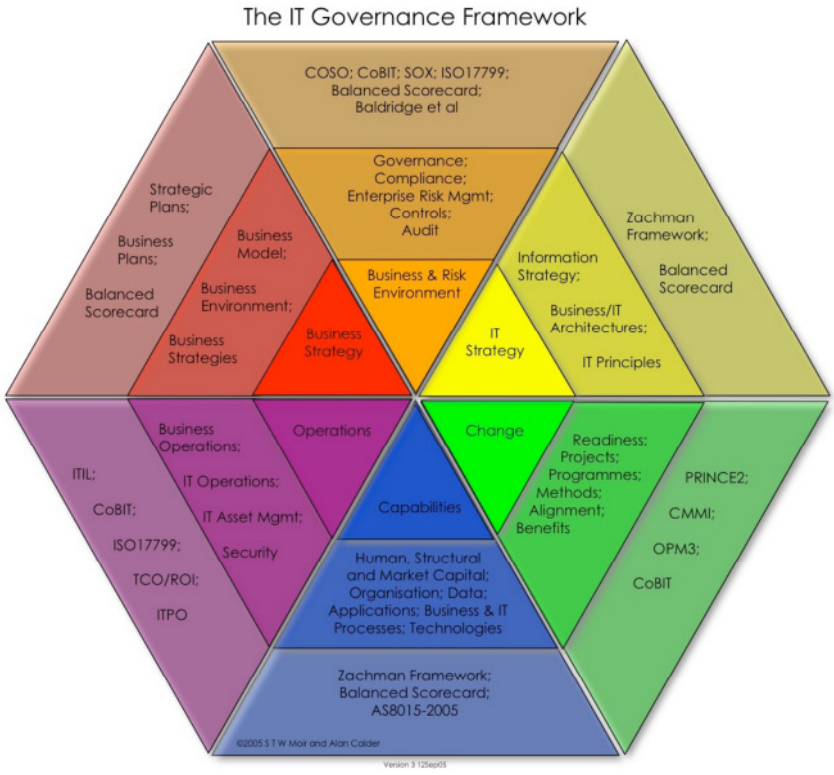


Figure 5: Calder-Moir Framework (Calder & Moir 2009)

2.2.3.2 ISO 17799 / ISO 27002 (IT Security)

ISO 17799 / ISO 27002 define guiding principles for the implementation of information security. These principles are based upon regulatory requirements and generally accepted best practices. Regulatory requirements are the protection of personal data, sensible organizational information and intellectual property rights whereas best practices contain information security policies, assignment of responsibility for information security, problem escalation and business continuity management (IT Governance Institute, 2008a). Data security and data privacy can play key roles in disaster management. In terroristic scenarios, secure information flows mission critical. An initial terroristic attack might not have severe consequences, but knowing the "security flaws" in the system can enable terrorist to do even more harm in a second wave (Kerr, 2003).

Even though ISO 17799 / ISO 27002 are not intended for use in counterintelligence for cybercrime and terrorism, they might be able to give a public organization guidance to install baseline security procedures and therefore prevent or mitigate the effect of a security breach or data theft. However, ad-hoc disaster situations might call for an "open communication" between organizations and data channels need to be established between organizations and authorities to master a serious situation. Therefore, a security model for disaster management needs to provide both, security and flexibility. Most tools and frameworks in IT Management rely on maturity models to "measure" their level of process implementation. A shared and standardized maturity model of security might give independent organizations a tool to trust each other to a certain level, even in ad-hoc situations, and consequently enable them to establish information and communication links to share mission critical information.

2.2.3.3 CMMI

The development of the Capability Maturity Model Integration (CMMI) has been started by the Software Engineering Institute (SEI) in the mid-1980s. The latest version of the CMMI is version 1.2 and has been released in August 2006. The objective of CMMI is to improve usability of maturity models for software

engineering, by integrating many different models into one framework (Software Engineering Institute, 2008).

“CMMI (Capability Maturity Model Integration) is a process improvement maturity model for the development of products and services. It consists of best practices that address development and maintenance activities that cover the product lifecycle from conception through delivery and maintenance” (Software Engineering Institute, 2006, p. 1).

CMMI represents a set of recommended practices for key processes, which have been used to enhance software process capability. It is a collection of best practices for Project Management, Software Engineering, Process Management and Support Processes to effectively manage software requirements, development, delivery processes and software quality. The CMMI provides a practical framework to organize evolutionary steps into five maturity levels and is compatible to the maturity levels of COBIT and ITIL.

Most benefits of CMMI come from its rigorous rating processes. With a maturity model the status of each process can be ranked from non-existent to optimized (0-5). This creates a measure for where the organization is in reference to its goals and in comparison to other companies. Maturity models also help to identify where improvements can be made (Software Engineering Institute, 2006).

With regards to trust, data protection and security, CMMI provides guidance for efficient and effective improvement across multiple process disciplines in the organization, but due to its focus on software development CMMI has its limitations on IT Service Management components such as infrastructure or more generic processes. One of the biggest criticisms is that implementing CMMI becomes too bureaucratic and time consuming (Software Engineering Institute, 2006; Wilkie, McFall, & McCaffery, 2005).

2.2.3.4 COBIT

Controlled Objectives for Information and related Technology (COBIT) is a well-known framework for IT Governance. COBIT enhances risk mitigation, IT value delivery and strategic alignment (Debreceny, 2006; Guldentops, 2003; Larsen,

Pedersen, & Andersen, 2006; Ridley, Young, & Carroll, 2004; Van Grembergen, et al., 2003). It links Business Requirements, IT Resources, and IT Processes, as shown in Figure 6.

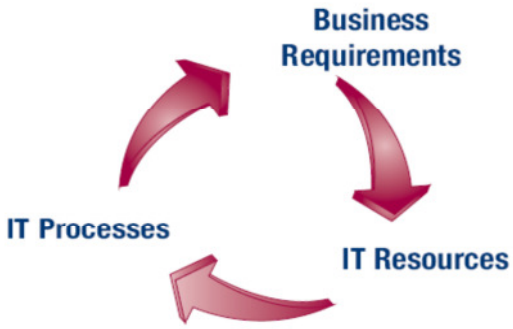


Figure 6: COBIT process (IT Governance Institute, 2007b, p. 21)

COBIT is built on four domains (Plan & Organize, Acquire & Implement, Deliver & Support, and Monitor & Evaluate) which are split into 34 manageable processes (IT Governance Institute, 2007b). In addition to the full COBIT implementation a COBIT Quickstart Edition exists, which is reduced in complexity and suitable for smaller companies (IT Governance Institute, 2007a). Each process consists of a number of activities and control objectives, each with its own metrics such as key performance indicators (KPI), key goal indicators (KGI), and critical success factors (CSF). Each process is assessed by a maturity model, which is related to CMMI. COBIT also provides a chart for the different processes and activities that recommends particular positions within an organization to be responsible, accountable, consulted, and informed (RACI chart). COBIT is an internationally recognized de-facto standard in IT Governance. Its current version is 4.1, but Version 5.0 will be published end of 2012 incorporating two other frameworks, Val IT and Risk IT, which are also described in in this chapter (Salle & Rosenthal, 2005; Simonsson & Hultgren, 2005; Simonsson & Johnson, 2006).

2.2.3.5 Val IT / Risk IT

Val IT and Risk IT are currently extension frameworks to COBIT 4.1. The close relation to COBIT is also reflected in Val-IT's and Risk IT's structure. However, their current versions can be used without a prior implementation of COBIT. In

COBIT 5.0 both frameworks (Val IT & Risk IT) will be implemented and will discontinue to exist as separate frameworks (IT Governance Institute, 2010a).

Val IT "focuses on the investment decision … and the realization of benefits ..., while COBIT focuses on the execution…" (IT Governance Institute, 2006a, p. 7). Even though its roots are in COBIT, a mature IT Governance framework, literature or extensive case studies about the Val IT are still forthcoming (Symons, Orlov, & Sessions, 2006). However, the ITGI and other researchers are constantly developing the framework and document related work to show the effectiveness of Val IT. To date they have published three additional papers to their framework: "The Business Case" (IT Governance Institute, 2006b), "The ING Case Study" (IT Governance Institute, 2006c) and "Value Governance – Police Case Study" (IT Governance Institute, 2007c). The latter paper demonstrated the successful applicability of the Val IT framework in public organizations by mapping and weighting IT projects in relation to public goals. The Val IT framework in its 2nd version consists of three major processes: Value Governance, Portfolio Management and Investment Management (IT Governance Institute, 2008c).

Risk IT is "a set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk" (IT Governance Institute, 2010b, p. 1). It helps to align enterprise risk with IT risks, while keeping its focus on the business perspectives and balancing the cost and benefits of IT risk management. It supports board managers to understand IT risk and allows them to make risk-aware decisions about an IT investment. The Risk IT framework in its first version is divided into three domains: Risk Governance, Risk Evaluation, Risk Response (IT Governance Institute, 2010b).

2.2.3.6 ITIL

ITIL has become the worldwide de-facto standard in IT Service Management (ITSM). A main advantage of ITIL is its provision of a common language for the IT and business departments to get faster and better benefits from their IT services (Böttcher, 2008; Van Bon & Verheijen, 2006). ITIL v2 is a widely used frame work to improve the service delivery of IT however, since May 2007 ITIL v3 was launched and updated much of the former domain "Service

Management". ITIL v3 includes five core books as shown in Figure 7 (IT Service Management Forum, 2009b):

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

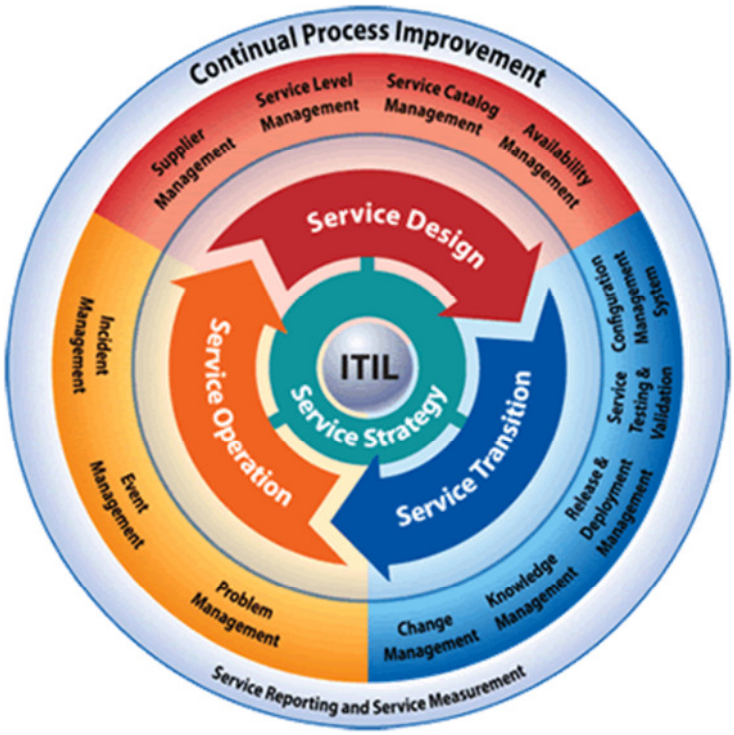


Figure 7: ITIL v3 (IET-Solutions, 2008)

In contrast to COBIT, ITIL focuses not on "WHAT" an organization should do to achieve alignment, it focuses more on the "HOW" IT can provide an aligned service to the business. The ITSMF defines that "a service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks" and "Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services" (Böttcher, 2008; IT Service Management Forum, 2009b).

In order to address smaller companies and organizations ITIL has, been adapted by a few researchers, to create a simpler version of an ITSM framework most commonly known as "ITIL Lite", "ITIL Small Scale", and

“Innotrain-IT”. Even though, these simplified versions are not an official ITSMF publication they show promising results in their areas and could also be suitable for small and medium EM organizations in an adapted version (Fry, 2010, 2011; Küller, Vogt, Hertweck, & Grabowski, 2011; Vogt, Küller, Hertweck, & Hales, 2011).

In addition to ITIL there are also a few proprietary service management frameworks out on the market. However, they are all based on or related to ITIL, such as the Microsoft Operations Framework (MOF), Hewlett Packard’s ITSM Reference Model (HPITSM) or IBM's Process Reference Model for IT (PRM-IT) (Van Bon & Verheijen, 2006).

2.2.3.7 ISO 20000 (IT Service Management)

On basis on ITIL the two leading ITSM organizations, IT Service Management Forum (ITSMF) and the British Standard Institute (BSI), created an internationally recognized and accepted standard (ISO 20000), which reflects the overall expectations of an IT organization. Therefore, the ISO 20000 standard is a subsequent development of the British Standard BS 15000 and is building a bridge between ITIL and COBIT (IT Governance Institute, 2008a; IT Service Management Forum, 2009a).

Prior to ISO 20000 it was not possible for organizations to become ITSM certified even though ITIL and COBIT have been successfully implemented. Now, it is possible to become an internationally accepted certification equally to the quality standard ISO 9000.

ISO 20000 is split into two parts (IT Service Management Forum, 2009b):

- Part1: Specification. This part describes the exact requirements which are mandatory in order to become certified
- Part2: Code of Practice. This part is offering best practices to fulfil the requirements of part 1, but they are not mandatory and can be adapted as long as they fulfil their purpose.

As mentioned ITIL (particularly version 3) is aligned with ISO 20000. Therefore its best practices and guidelines fully comply with the ISO 20000 requirements (Kempter & Kempter, 2009).

2.2.4 Contribution of IT Governance to Public Organizations

A critical factor for an organization's success is to obtain a competitive advantage, which is generally the source for growth. If IT is aligned with business goals, it can deliver important strategic advantages and helps an organization to become more efficient (Weill & Ross, 2004).

Even though organizations within the domain of Emergency Management have no need to gain competitive advantage, they have a responsibility towards the society to do their best to save lives and critical infrastructures. Thus, they have to react faster and make better decisions. IT can help to gain that edge. Emails, Geo Information Systems (GIS), Global Positioning Systems (GPS), Business Intelligence (BI), Video Conferences, Workflow Systems, etc., all these technologies have the capability to assist Emergency Management teams before, during and after an incident. However, they need to be managed to provide reliable, secure, and appropriate services. Investing in wrong IT systems and projects, due to the unawareness of technological opportunities and risks, as well as unreliable information systems and slow communication channels, can be the cause of casualties and large scale destruction (Dilmaghani & Rao, 2009; Rao, et al., 2007).

Previous research projects have shown that IT Governance tools can contribute to support public organizations in their daily work if they are adapted towards their needs (Di Maio, 2003a, 2003b, 2007; IT Governance Institute, 2003; Sethibe, Campbell, & McDonald, 2007; Vogt & Hales, 2010). Therefore, this research will show how IT Governance and its mechanics can also be applied to the domain of Emergency Management.

2.3 IT / IS and its Management in the Domain of Emergency Management

Information Technology (IT) and Information Systems (IS) are emerging disciplines in the domain of Emergency Management and are still in their infancy. Compared to other disciplines the available literature is scarce. The available publications usually focus on supporting technologies (GPS, GIS, CIMS, Early Warning Systems, etc.) and decision making during an emergency

situation, but IT Management issues have been neglected. Only a couple of researchers have attempted to explore this area.

First investigations towards the utilization of IT Management and governance methods were done by Van Den Eede and Van de Walle (2005). They explored the cross-fertilization and benefits of IT Governance methods for Information Systems for Crisis Response and Management (ISCRAM). They came to the conclusion that mainstream methods in IT Governance can have positive effects on ISCAM but due to the different structures and needs in Emergency Management further research is needed (Van Den Eede & Van de Walle, 2005).

In 2005 Wang & Belardo wrote an article about strategic integration of knowledge management in crisis management. Even though they concentrated on knowledge management, they also discussed basic issues and benefits of "strategic alignment" in their paper. They concluded that there is a need for organizations to establish an understanding of what they really need in order to be better prepared, but the unpredictable nature of disasters is a problem for conventional methods. Thus, relating to strategic IT alignment they concluded that although this is a proven method in business it needs to be determined whether IT alignment and Emergency Management strategies will also improve the organizational performance in EM (Wang & Belardo, 2005).

Dwarkanath & Daconta (2006) wrote an article about Service Oriented Architecture (SOA) in Emergency Management. They concluded that in order to design a SOA for Emergency Management enterprises, the overlaying governance component needs to be agile and flexible to accommodate the diverse stakeholders and their interests, the different business processes, and in order to be successful, it must provide transparency. In their perspective alignment in Emergency Management needs special attention but it is not achievable with conventional methods (Dwarkanath & Dakonta, 2006).

In the meantime (2005 – 2007) the United States Federal Emergency Management Agency (FEMA), conducted an extensive research project to identify the role of IT in disaster management. Roa et.al (2007) found out that IT has yet unrealized potential in the domain of EM, but decision makers in EM

organizations lack the clarity of a vision how new technologies can be applied in their routines. A method to assess and prioritize IT investments according to their risk and opportunities is needed to realize benefits and improve EM processes in most EM organizations.

In 2007 Iannella et al. discussed a framework towards the development of crisis information management systems (CIMS). Though concentrating on system development guidelines they also examined the needs and requirements for IT in disaster management and identified that stakeholders in Emergency Management are moving towards efforts to define and exploit greater IT utilization during major incidents. In their perspective, "... Emergency Management is not a discipline that follows well behaved rules and allows itself to be modelled sufficiently well that all contingencies can be catered for a priori" (Iannella, et al., 2007, p. 1). As a result, information management strategies diverge depending from the phase, severity, and kind of disaster. Thus, they argue that Emergency Management is still in its infancy when utilizing IT solutions and common tools, frameworks, and terminologies are needed. (Iannella & Henricksen, 2007; Iannella, et al., 2007).

Marich, Horan, & Schooley (2008) examined the inter-organizational IT Governance structure by the means of a case study performed at a Medical Emergency Service Agency in California. The aim of their research was to analyse inter-organizational information flow by a standardized framework. Their findings confirmed that a shared and standardized IT Management framework and standardized interfaces have advantages in inter-organizational information flow.

More recently Weyns & Höst (2009) have picked-up the topic of IT Management and governance and investigated a maturity model for Swedish municipalities to measure their IT dependability in disaster situations. They have interviewed emergency managers and responsible IT managers in two large Swedish municipalities. Their conclusions confirmed FEMA's findings that there is a large gap between IT personnel and emergency managers. They conclude that most inefficiencies, mistrust in IT and misalignments exist because there is no valuable interaction between the two functions. Hence, the general IT maturity is rather low (Weyns, Höst, & Helgesson, 2010).

Harrald (2011, p. 1) spoke about “achieving agility in disaster management” utilizing IT systems. Based on his previous research about 9-11 and Hurricane Katrina (Harrald, 2006), he concluded that the domain of Emergency Management requires “the agility desired by the social sciences and the discipline created by the professional practitioners”. He explored how agility can be developed in such a disciplined system and how “outcome based goals, adaptive leadership, and technology” can support EM organizations. As a result, one can conclude that not only operational processes and technologies need to be agile and but also the organizational structures and strategic alignment methods.

2.3.1 IT Related Requirements of Emergency Management organizations

2.3.1.1 High Reliably Theory

Emergency Management organizations are different from commercially driven organizations.

First, they are not financially driven. Their goal is not to make revenue or increase their market share but usually they are restricted to budget. Therefore, they can be considered as non-profit organizations (NPO) in the broadest sense. Second, they don’t have an “off-the-shelf product”. Their goals are quite diverse since a bush-fire demands different actions than a pandemic. Hence, their tasks are very different and the need for “Emergency Management” is highly volatile. Large-scale emergencies, disasters, and crises can usually not be predicted, at least not in way that all actions can be planned a priori. Nevertheless, their processes have to be highly reliable since lives and environment are at stake. For the latter Van Den Edee and Van de Walle (2005) have summarized required characteristics for High Reliability Organizations (HRO) in the following tables:

Complexity	
Characteristics	*Responses*
potential for unexpected sequences	continuous training
	Redundancy
complex technologies	continuous training
	responsibility and accountability at all levels
potential for systems serving incompatible functions to interact	job design strategies to keep functions separate
	Training
indirect information sources	many direct information sources
baffling interactions	training of specialized language
	flexible exercises

Table 1: Characteristics of EM organizations and responses (Van Den Eede & Van de Walle, 2005, p. 55)

Tight coupling	
Characteristics	*Responses*
Time dependent processes	Redundancy
invariant sequences of operations	job specialization
	system flexibility hierarchical differentiations
Only one way to reach goal	Redundancy
	system flexibility
Little slack	bargaining and negotiation
	system flexibility

Table 2: Characteristics of EM organizations and responses (Van Den Eede & Van de Walle, 2005, p. 56)

These tables explain how High Reliability Theory (HRT) deals with the objections of Normal Accidents Theory (NAT) concerning complex and tightly-coupled systems. NAT stresses that whatever organizations do, accidents and failures will happen in complex, tightly-coupled systems. On the other hand, HRT asserts that organizations have an influence on the reliability (Rijpma, 1997; Roberts, 1990; Van Den Eede & Van de Walle, 2005).

Even though these theories are sometimes contra dictionary, both theories illustrate the unique requirements of EM organizations and corresponding requirements of IT systems and IT Management.

2.3.1.2 DERMIS Approach

The Dynamic Emergency Response Management Information System framework (DERMIS) developed by Turoff, Chumer, Van de Walle and Yao (2004) describes a set of general and supporting design principles and

specifications, which should be considered when designing an information system (IS) for EM organizations. They suggest nine design premises complemented by a series of five design concepts, eight general design principles, and three supporting design considerations as shown in the following table:

A. Design Premises 1. System Training and Simulation 2. Information Focus 3. Crisis Memory 4. Exceptions as Norms. 5. Scope and Nature of Crisis 6. Role Transferability 7. Information Validity and Timeliness 8. Free Exchange of Information 9. Coordination	**C. General Design Principles and Specifications** 1. System Directory 2. Information Source and Timeliness 3. Open Multi - Directional Communication 4. Content as Address 5. Up-to-date Information and Data 6. Link Relevant Information and Data 7. Authority, Responsibility, and Accountability 8. Psychological and Social Needs
B. Conceptual Design 1. Metaphors 2. Human Roles 3. Notifications 4. Context Visibility 5. Hypertext	**D. Supporting Design Considerations and Specifications** 1. Resource Database and Community Collaboration 2. Collective Memory 3. Online Communities of Experts

Table 3: DERMIS Design Model (Turoff, et al., 2004, p. 4)

Even though the DERMIS approach cannot be applied completely in order to design a domain specific IT Governance method, it provides useful guidelines, which should be considered. Thus, the following principles are seen as important for the design of such a method:

- "**Premise 1 - System Training and Simulation:**

  An emergency system that is not used on a regular basis before an emergency will never be of use in an actual emergency (Turoff, et al., 2004, p. 6)." If an information system is only used in one particular emergency situation it is quite likely that staff is not familiar with it and will avoid using it. Hence, the researcher suggests that IS systems should not be aligned to emergency situations but rather to often reused processes or patterns of actions (in the IVEM² method (see chapter 9.3) these will be referenced as 'modules'). This would "force" EM staff to use systems regularly.

- "**Premise 4 - Exceptions as Norms:**

  Almost everything in a crisis is an exception to the norm (Turoff, et al., 2004, p. 8)." IT Governance processes and IT value estimation methods have to cope with uncertainties. Processes have to be flexible and value estimation methods need to consider uncertain factors. Again, strictly predefined emergency situations seem to be counterproductive in this case. New methods need to find ways that are more agile.

- "**Premise 6 - Role Transferability:**

  It is impossible to predict who will undertake what specific role in a crisis situation. The actions and privileges of the role need to be well defined in the software of the system and people must be trained for the possibility of assuming multiple or changing roles (Turoff, et al., 2004, p. 8)." Therefore, it is paramount that IT Governance models in EM consider ad-hoc teams, flexible inter-organizational collaboration, and changing responsibilities due to escalation levels. Such conditions are rather unusual for regular businesses with off-the-shelf products and not considered in existing IT Governance and ITSM frameworks.

- "**Premise 9 – Coordination:**

  The crux of the coordination problem for large crisis response groups is that the exact actions and responsibilities of the individuals cannot be pre-determined (Turoff, et al., 2004, p. 10)." Considering the "Decision Matrix" and "IT Governance Archetypes" developed by Weill & Ross (2004), IT decision rights need to take shifting responsibilities in account. High volatilities in hierarchies and organizational structure are usually not found in industry. Hence, IT Governance methods need to be adapted accordingly for the EM domain.

EM organizations are High Reliability Organizations (HRO), which need individual design premises; hence, a proposed IT Governance framework for EM organizations should be able to cope with:

- Unexpected situations
- Flexible processes

- Different information channels
- Organizational and hierarchical issues
- Limited financial resources

… and give support to:

- Identify the most valuable IT initiatives
- Reduce risk of IT initiatives and associated operational processes
- Provide a highly reliable infrastructure even in uncertain environments

2.3.2 IT Governance Frameworks in Relation to Emergency Management

Since previous research projects have identified that IT Governance frameworks and methods need to be adapted for non-commercial organizations (Di Maio, 2003a, 2003b, 2007; IT Governance Institute, 2003; Sethibe, et al., 2007; Vogt & Hales, 2010) it can be concluded that these frameworks also need to be adapted for the domain of Emergency Management.

It was clear to the researcher that multiple IT Governance and ITSM frameworks exist but due to time and resource constraints a selection had to be made early in this research project. However, as described in one of the previous sections and from experience with previous research projects the two leading frameworks (ITIL and COBIT) provide a good basis for a domain specific IT Governance approach.

Di Maio (2003b) and Sethibe's et al. (2007) identified that IT Governance structures and goals in public organizations, which EM organizations usually are, differ from private sector. In private organizations IT investments are usually aligned with business goals such as revenue, market share, cost, turn-over rates, etc. Public organizations usually follow non-monetary goals such as political goals, charity, community safety, etc. Hence, monetary driven tools such as ROI, NPV and BVIT are not as valuable for the non-profit sector. Nevertheless, these methods are frequently used even though they have misleading results, which need to be "manually" adjusted to fit community interests and political goals (Vogt & Hales, 2010). In addition to these previous research projects, the researcher has identified other issues in EM

organizations, which are not properly addressed by existing IT Governance frameworks and IT value estimation methods.

1. They cannot deal with uncertainties, such as the variety of EM situations, different severity of impact and changing probability of occurrence.
2. They cannot deal with multi organizational structures (ad-hoc teams), which are very common during emergency situations.
3. They are often seen as too complex by Emergency Managers. The rigor and broadness of these frameworks does often not allow the flexibility needed in EM situations.
4. They do not give an exact guidance. Particularly COBIT and Val-IT give good guidance about "what" to do, but they don't say "how" to do it.
5. The full implementation of a framework can overburden small & medium EM organizations. Domain specific adaptations of these frameworks might be more appropriate.

As an example for these issues one can have a look at COBIT's control objective PO5 (Plan & Organize – Manage the IT investment). The COBIT framework suggests the following (IT Governance Institute, 2007b, p. 47):

"Control over the IT process of
Manage the IT investment
that satisfies the business requirement for IT of
continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions
is achieved by
• Forecasting and allocating budgets
• Defining formal investment criteria (ROI, payback period, NPV)
• Measuring and assessing business value against forecast
and is measured by
• Percent reduction of the unit cost of the delivered IT services
• Percent of budget deviation value compared to the total budget
• Percent of IT spend expressed in business value drivers
(e.g., sales/services increase due to increased connectivity)"

Doubtlessly, the PO5 gives good guidance on how to manage IT investments and build a sound IT portfolio. However, its focus lies fully on monetary measurements and does not incorporate "intangible" goals and changing circumstances. In addition, an IT portfolio according to PO5 would not be able

to deal with “uncertainties” and “ad-hoc teams”. First, value predictions and portfolio prioritizations are based on complex and expensive business cases. However, EM situations are mostly diverse and cannot be fully foreseen. Second, in case of a large emergency there are usually multiple organizations involved. PO5 does not consider an overarching IT portfolio between these organizations to gain leverage effects (such as improved communication and data sharing during an emergency) or synergetic advantages of ad-hoc teams (such as sharing on-site infrastructure from other EM organizations). Its focus is tailored to private organizations, which usually work on their own.

Since this research is concentrating on Strategic IT Alignment, the project is limited to the following frameworks:

- COBIT 4.1
- ITILv3

The limitation was based on the holistic concept of both frameworks and their high acceptance rate in commercially driven organizations. Additionally, ITILv3 and COBIT 4.1have a strong strategic focus but also consider operational processes.

2.4 Discussing the Literature

Literature has shown that IT Management and IT Governance are still in their infancy in the domain of Emergency Management. However, IT has been identified as one of the most promising approaches to improve disaster management processes. Appropriate technologies, information systems, and IT services can improve information richness and reach, as well as availability and quality, and therefore enable emergency managers and first responders to react faster and more precise. On the other hand, unmanaged IT infrastructures and inappropriate technologies bear unknown risks and can jeopardize all attempts to prevent and mitigate threatening situations or rescue people in danger. Leading Emergency Management specialists say that IT Management approaches, which meet the demands of disaster management are urgently needed (Iannella, et al., 2007; Rao, et al., 2007; Weyns & Höst, 2009).

Even though there are initial approaches to investigate the influences of IT Management and IT Governance methods in the domain of Emergency Management, it is clear that there is insufficient research in this area. The issue of aligning IT initiatives with unpredictable situations, such as disasters, is yet unsolved. Even though high reliability concepts exist (HRT / NAT), which can be used to develop appropriate information systems, the successful governance, management, and value preservation of these information systems and underlying IT infrastructures seems to be immature. Moreover, EM operations seems to have only little trust in IT enabled processes. Consequently, IT Governance and IT Service Management have not yet unfolded their full potential in the domain of Emergency Management (Rao, et al., 2007; Van Den Eede & Van de Walle, 2005; Wang & Belardo, 2009).

Even though there are existing frameworks and methods such as ITIL, COBIT and Val-IT, strategic IT alignment is yet a challenging task even in industry. Considering the fact that Emergency Management has to deal with uncertainties, multi-agency collaboration, and ad-hoc situations on a regular basis this task is even more challenging. However, EM organizations realize the general potential of IT to support their actions, but value and reliability are unclear. Domain specific IT Governance methods have been successfully applied in other domains to overcome such issues. Hence, it is the researcher's belief that an EM specific IT Governance model is the right step into the right direction. Such a conceptual model can be used as a reference for EM organizations to improve their IT enabled processes and realize value from future IT initiatives and existing IT services.

The most supporting statements for this research project are the results from the United States Federal Emergency Management Agency (FEMA) (Rao, et al., 2007) as well as a more recent research in Swedish municipalities (Weyns & Höst, 2009). Both studies have identified IT Management issues and lack of understanding of IT values and risks. Thus, one can say that IT Management and IT alignment issues are of concern to most Emergency Management organizations, which is supported by results of the researchers own data collection and analysis (see Part II). In addition to their view about IT Management and IT alignment issues, Harrald's (2011) statements about

“agility in disaster management” and Turoff et al. (2004) DERMIS approach directed this research towards the question “how can EM organizations align their IT initiatives and be prepared for the unknown”. Particularly some of Turoff et. al “design premises” seem to be most appropriate to design a flexible and reliable IT Governance method for EM organizations since they have been successfully applied in other research projects (Van Den Eede, Muhren, Smals, & Van de Walle, 2006).

The following chapters will therefore describe the development process of a conceptual and domain specific IT Governance approach for Emergency Management organizations. They will illustrate the research structure, research methodology, data collection, data analysis, and the modelling / design of the three main IT Governance components of this conceptual reference model.

PART II:
Research Structure & Methods

3 Research Structure

3.1 Research Question & Research Gap

After the literature review and research gap identification a general research question was formed, which guided the researcher throughout this project:

“How can Strategic IT Alignment in Emergency Management organizations be improved to get most value out of IT initiatives and consequently achieve better emergency preparedness?”

Since this problem is rather universal and complex, this thesis will concentrate on three underpinning questions: First ‘evaluation and adaptation of existing IT Governance frameworks and processes’, second ‘organizational changes and IT decision rights’, and third ‘IT value estimation in uncertain environments’. The following diagram (Figure 8) will explain this process briefly:

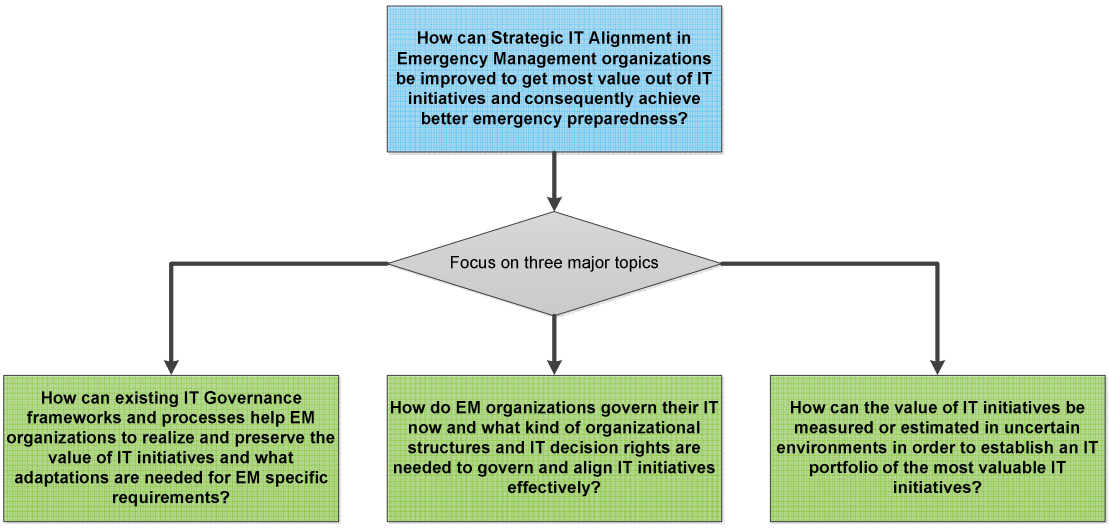


Figure 8: Research Questions

The decision to divide the general research question into three sub questions was made because these questions mainly influence strategic IT alignment within an organization. Focusing only on one of them would cause an imbalance since IT Governance process cannot be successfully implemented without the support from the right key stakeholders, and an optimized IT decision matrix with a limited IT value estimation method will not achieve

strategic IT alignment either (Project Management Institute, 2008; Weill & Ross, 2004).

Therefore, this research investigated in these three directions in order to deliver the following:

1. Identify control objects and processes from existing IT Governance frameworks and generate a simplified and domain specific framework
2. Identify general organizational and process issues from the As-Is models of the case studies and provide a guideline for suitable IT decision archetypes and mediating functions
3. Find an IT value method that can cope with the uncertain nature of large-scale emergencies, disasters, and crises
4. In a final step, combine the three sub-items and define a conceptual and domain specific reference model that incorporates the IT value estimation method, deals with the identified organizational issues and uses domain specific IT Governance processes based on existing frameworks.

In order to answer these questions, the research project is limited to the prevention and preparation phase as described in chapter 2.1.3 and Figure 1 (p.30) since both phases seem to be the most promising stages to make strategic IT decisions. Nevertheless, all actions taken in these phases will have to consider the needs of following stages since they will be influenced largely by the prevention and preparation phase. Particularly the response phase will be affected since IT enabled EM processes are based on a well-functioning IT infrastructures. Hence, this research will also discuss some of the transitional stages where IT strategy will blend into IT operations.

Since the research gap contains social and technological elements the resulting research questions are rather complex. Addressing these questions with quantitative approaches only would not be suitable since such an approach would only be able to cope with the different and rather unstructured data resources. However, socio-technical problems demand a research method, which is able to combine different views on the problem in order to reflect its complexity (Cole & Avison, 2007; Frank, 1999; Gable, 1994; Klein & Myers,

1999; Myers, 1997, 1999, 2008). Thus, it became clear that the researcher has to focus on qualitative research methods to achieve the best and most meaningful results. According to the researchers cited above, qualitative research methods are most suitable to address managerial issues such as strategic IT alignment and IT Governance. Hence, it is the researcher's belief that a qualitative research approach is the best choice to answer the research questions and design new models and methods for the EM domain. A more detailed discussion about the choice and limitation of the research approach can be found in chapter 4.

3.2 Research Contribution

The aim of this research project is to develop models and methods to align IT initiatives with Emergency Management processes and successfully transfer these IT initiatives to reliable and efficient IT operations. The models, processes, and methods will be tailored for authorities and NGOs that take part in the event of a major emergency or disaster.

The research project identified special requirements of the EM domain, by the means of case studies and interviews conducted in Australian and German organizations. Results of the data collection phases highlighted the major issues of EM organizations with regard to IT Governance and IT Service Management. Furthermore, it investigated and demonstrated the usability and limitations of existing IT frameworks in the Emergency Management domain. Based on these findings the researcher has developed

- a simplified IT Governance process catalogue based on the most common IT Governance frameworks (ITIL & COBIT),
- identified organizational issues and has suggested corresponding IT decision rights and mediating functions,
- developed an IT value estimation method, which is capable of building an IT portfolio that can cope with uncertain situations to a certain degree
- and finally combined these to conceptual reference model.

The goal of this research was to provide a holistic IT Governance method that will help EM organizations to assess and improve their IT processes and make the right IT investments. The conceptual reference model should assist authorities and NGOs to improve their overall emergency preparedness and disaster response processes. Aligned IT services, which can be used even in yet unknown situations, will help them to react faster and become more efficient. Reliable IT services will increase the trust in IT enabled processes and foster the utilization of IT in this domain. Shared IT decision rights and conjoint agreements within and between organizations will help to improve information exchange and streamline EM processes.

3.3 Research Limitations

Due to the rather complex and multidisciplinary topic of Emergency Management in association with IT Governance methods, the research is based mainly on qualitative research methods. The researcher was aware that the data collection can yield additional questions (such as sociological and political issues), which cannot be covered fully in this research project due to limited time and resources. Therefore, this research will ignore issues, which are not directly associated with IT Governance. Hence, private, political, social, and hierarchical discordance is deliberately neglected.

Only Australian and German organizations have been used as primary data sources since they were directly accessible to the researcher. Nevertheless, findings from published case studies or official reports have been used as secondary data sources and have been integrated into this research project to increase the general applicability of the conceptual models and methods.

Since the data collection and analysis was limited due to restrictions of the researched organizations and the relative small number of participants, only a conceptual reference model in an assumed “perfect world” could be designed. Applying a new theory in a real environment was too delicate for the participating EM organizations. Therefore, the final model was tested on a theoretical basis only. However, experts in the field have evaluated the conceptual models and methods and compared them to existing procedures in

EM organizations they work with. They reviewed the conceptual model against current processes and tools by the means of a survey and thus identified where the new models and methods are superior or inferior compared to their current procedures.

It is evident that the final results regarding the efficiency and effectiveness of the model can only be confirmed in a long term study, where the model is implemented step by step in operational procedures of an Emergency Management organization. Therefore, the evaluation results can only be seen as an indicator for the possible improvements of this concept and findings of this thesis are limited to a conceptual stage only. Nevertheless, the models and methods have been applied to a cases study in chapter 10 to proof their applicability. However, further research will have to prove the model in the field but due to the lengthy process of such an implementation and the lack of available resources, this was excluded with respect to this thesis.

4 Research Design

4.1 Epistemological Foundation

Epistemology comes from the Greek and can be translated as “study of knowledge” and refers to the assumptions about knowledge and how it can be collected and gained (Hirschheim, 1992; Myers, 1997, 2008). However, epistemological paradigms have been defined in different ways.

Guba and Lincoln (1994) defined four categories:

- positivism
- post-positivism
- critical theory
- constructivism

Chua’s (1986) suggests only three categories (see Figure 9):

- positivist
- interpretive
- critical

It is not the intent of this thesis to discuss the different views of the mentioned researchers. From the perspective of this particular research project, Chua’s model seemed to be sufficient to define the underlying epistemological approach. Hence, the following paragraphs will briefly explain the used model.

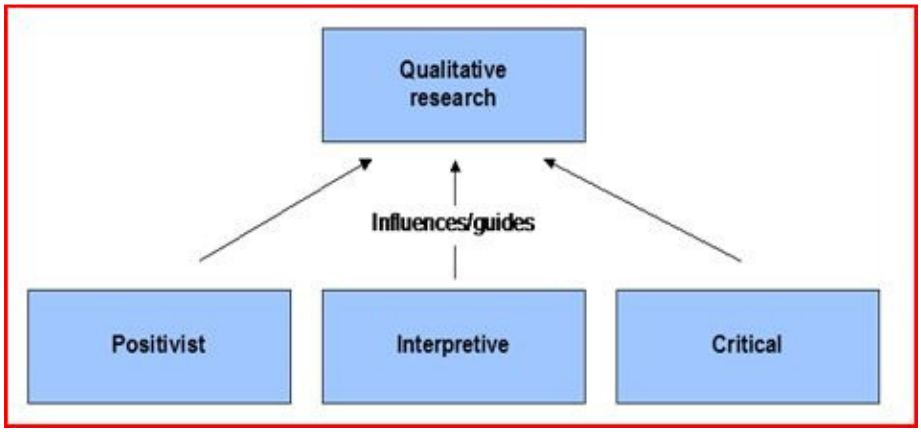


Figure 9: Epistemology model (Chua, 1986; Myers, 2008)

4.1.1 Positivist Research

Positivists say that reality is given and objective. Therefore, it can be described by measurable indicators, which are independent of a researcher's view and should therefore yield identical and reproducible results. Positivists commonly attempt to test hypotheses and use data to either falsify or support it (Myers, 1997, 2008). However, Leimeister (2010, p. 10) states in her thesis that "a single-focused view of the positivist perspective has been attenuated and replaced in recent years with the recognition that eventually all measurement is based on theory and therefore capturing a truly objective truth is impossible."

Orlikowski and Baroudi (1991) studied numerous IS research projects and categorized them as positivistic if one or more of their criteria was met:

1. evidence of formal propositions
2. quantifiable measures of variables
3. hypothesis testing
4. the drawing of implications about a phenomenon from the sample to a stated population.

Therefore, IS research is often defined as positivistic if the research is referring to schemas, quantifiable measures of variables, hypothesis testing, and conclusions which can be drawn from a single sample to a defined group (Myers, 1997, 2008).

Positivism has been the major epistemological paradigm in IS research until the 1990s. However, researchers have begun to discuss its relevance even though, or rather because, it uses rigorous research methods. The discussion is known as the "Rigor vs. Relevance" debate (Benbasat & Zmud, 1999; Davenport & Markus, 1999; Lee, 1999). Moreover, Frank (2003) raises an argument that positivistic driven research is often neglecting the actual research objects, applicability of scientific results and creation of new ideas due its focus on rigidity.

4.1.2 Interpretive Research

In contrast to the positivistic approach, interpretive research is assuming that access to reality can only be retrieved by social constructions such as

language, consciousness, and shared meanings. Interpretive research is often based on hermeneutics and phenomenology, which are methods that can help to understand the objective of the research through statements and behaviours of people and the researcher's interpretations of their meaning (Boland, 1985; Myers, 1997, 2008). Using the interpretive research paradigm provides detailed insight into "the complex world of lived experience from the point of view of those who live it" (Schwandt, 1994, p. 118), whereas the researcher becomes the means by which this reality is revealed (Andrade, 2009; Walsham, 1995a, 1995b).

In the information systems science these methods are applied to produce "an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (Walsham, 1993, pp. 4-5).

It can therefore be said that interpretive research does not predefine dependent and independent variables, which can be tested to falsify or support a hypothesis, but focuses on the full complexity of human sense making as the situation emerges (Kaplan & Duchon, 1988; Kaplan & Maxwell, 1994; Myers, 1997, 2008).

Constructivism as part of interpretive research is often applied in modelling (Frank, 1999; Pickard & Dixon, 2004). Frank (1999, p. 696) states that "the constructivist strategy aims at models of future worlds (for instance: models of information systems that are well integrated with a (re-) organized business)".

4.1.3 Critical Research

According to Popper (1980) research is critical when it tries to find weak spots in theories and their consequences. Others describe critical researchers as the assumption that social reality comes from experience and history (Held, 1980). Although people can try to change their social and economic circumstances their ability to do so limited by social, cultural, and political domination. Therefore, critical research is focusing on the oppositions, conflicts, and contradictions in our society and tries to break these boundaries (Myers, 1997, 2008). Critical research in IS follows the same paradigms as critical research in

general in order to illuminate restraining and isolating conditions and to be emancipatory (Hirschheim & Klein, 1994; Klein & Myers, 1999). Hence, it aims to expose the weaknesses and ambiguities within the area of research, which can be problems of IS, such as systems failure or resistance to systems (Wilson, 2003).

Critical research needs critical research methodologies, which involve the researcher and aim to change current realities. These methodologies could be most non-positivist methodologies, which are based on constructionism and the importance of discourses such as action research and qualitative research (Hirschheim & Klein, 1994; Ortmann, Windeler, Becker, & Schulz, 1990; Schultze & Leidner, 2002; Ulrich, 2001).

4.1.4 Discussing the Applied Epistemological Paradigms

Even though these research epistemologies are seen as distinct types, there is a discussion if the epistemologies can be mixed in a single research project (Myers, 1997, 2008). Flick (2002, p. 25) states that “different research perspectives may be combined and supplemented” if the research objective demands it, a statement which is supported by Pickard & Dixon (2004).

Following Flick’s (2002) and Pickard’s & Dixons (2004) advice it was decided to use different epistemological paradigms to tackle this multi-disciplinary research project.

The ‘interpretive’ approach, which demands qualitative research methods, was chosen as the leading epistemological assumption since it has been seen as the most suitable to understand how Information Systems (IS) and Emergency Management (EM) processes go together. Klein and Myers (1999) state that “interpretive research can help IS researchers to understand human thought and action in social and organizational contexts; it has the potential to produce deep insights into information systems phenomena including the management of information systems”.

However, also the ‘critical’ paradigm has been used to understand why IT Governance methods are not as highly accepted in the domain of Emergency Management as in industry. The critical view gave the researcher the ability to

identify gaps between the ‘as-is’ situation and the ‘should-be’ and allowed him to construct new concepts. Moreover, the combination of the interpretive and critical approach allowed the researcher to construct conceptual models to redesign traditional means of communication and cooperation using a constructive research strategy (Frank, 1999).

Finally, also the ‘positivistic’ view, often associated with qualitative research methods, has been used towards the end of the study to evaluate the findings from a different perspective and add more rigor to the research approach.

4.2 Research Methods

A research method is a strategy of how to tackle a research question. Coming from the underlying philosophical assumptions it defines the research design and data collection. Specific research questions demand different research methods (Krcmar, 1998). As with the underlying epistemological assumptions, the research’s objective can only be tackled by applying different research methods. The following sections will briefly describe the utilized methods.

4.2.1 Qualitative Research

According to Myers (1997, 2008) qualitative research methods have been developed in the social sciences to support researchers to study social and cultural problems or behaviours. Qualitative methods include action research, case study research, and ethnography, whereas the data for these methods can be retrieved from observations, interviews, questionnaires, documents, reactions of subjects, and the researcher's impressions and interpretations (Glaser & Strauss, 1967; Mayring, 2000, 2002; Myers, 1997, 2008). As the focus of information systems research shifts from technological to managerial and organizational issues, qualitative research methods have become increasingly useful (Gable, 1994; Klein & Myers, 1999; Myers, 1997, 1999, 2008).

4.2.1.1 Hermeneutics

The principles of hermeneutics reach back to the ancient Greeks. However, modern hermeneutics were developed during the 19th and 20th century and were first applied to information systems towards the end of the last century (Cole & Avison, 2007; Klein & Myers, 1999; Myers, 2008). Its theory is based on a social subjectivist paradigm where meaning is inter-subjectively created (Berthon, Pitt, Ewing, & Carr, 2002; Wong, 2005). Hermeneutics can be seen as both an underlying research philosophy and a tool to analyse rich, complex and unstructured data. Thus, it provides the ability to structure interpretations from unstructured material by suggesting a way of understanding textual data (Bleicher, 1980; Myers, 2008).

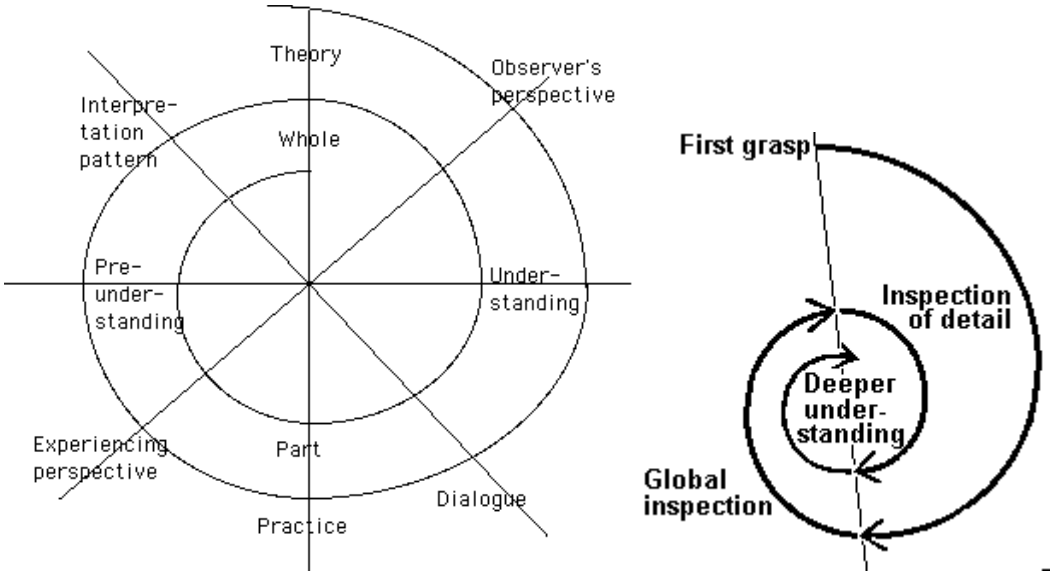


Figure 10: Hermeneutic Spiral a:(Rydberg Fahraeus, 2009) / b:(Routio, 2007)

The primary motivation to choose an interpretative research approach in IT is the belief that the understanding of a specific domain is retrieved by language, consciousness, and shared meaning (Cole & Avison, 2007; Klein & Myers, 1999). Several interpretive research approaches have been used in information systems research (e.g. ethnography and case study), but hermeneutics, though rather new in IS research, is most promising due to its universal applicability (Cole & Avison, 2007). Since hermeneutics is of interpretive nature, fixed criteria and automated calculations cannot be applied to retrieve meaning from unstructured sources (Cole & Avison, 2007; Klein & Myers, 1999; Wong, 2005). However, the method provides a meta-principle, known as the hermeneutic

spiral (Figure 10), which guides the researcher through the process of understanding and sense making. It “moves from parts of a whole to a global understanding of the whole and back to individual parts in an iterative manner” (Wong, 2005, p. 1). This meta-principle allows the researcher to understand and point out complex correlations and contradictions in order to develop a detailed general theoretical concept through abstraction and generalization (Cole & Avison, 2007; Klein & Myers, 1999; Wong, 2005).

4.2.1.2 Qualitative / Quantitative Content Analysis

Quantitative content analysis is a method developed in the early 20th century and is summarizing any type of content by measurable aspects of the content. This enables a researcher to be more objective than if the research would be based on the impressions of a listener. Classic content analysis, though it often analyses written words, is a quantitative method. The results of content analysis are numbers and percentages (Berelson, 1952; List, 2007). After doing a content analysis, a researcher might make a statement such as "82% of all emergency managers interviewed mentioned ‘alignment’ as one of their key issues". It may seem basic to make such statements, but the counting has two functions:

1. remove most of the subjectivity
2. detect trends

Mayring (2000), however, argues that quantitative content analysis neglects four important aspects, particularly when complex environments are analysed:

1. word counts cannot reflect the importance of the context
2. latent meanings
3. individual but striking cases
4. deliberately omitted statements

His attempt of ‘Qualitative Content Analysis’ (QCA) is to use the advantage of the conventional content analysis without being dragged into quantification schemes too fast. His approach is to summarize statements, look deeper in their meaning, and then build a categorization system and structure. These categories can then be linked with the identified statements and afterwards

quantified for further modelling and analysis. His approach was used in several successful information, communication, and management research projects and was therefore be chosen as the primary qualitative research method since it is able to incorporate secondary literature, documentation, interviews and case studies (Mayring, 2000, 2002).

4.2.1.3 Action Research

First mentioning of the term 'action research' was formed by Kurt Lewin (1946). According to him and Rapoport (1970), action research is comparative research, which involves collaboration from both the researcher and the subjects in order to analyse the effect of actions and reactions with regards to a specific problem. In contrast to applied social science, which just applies theories, action research tries to enlarge the body of knowledge by altering and improving applied theories by the means of a discourse an iterative action with subjects in the field.

Baskerville and Wood-Harper (1996, 1998) discussed the application of action research in information systems research and identified it as an appropriate method for this research area. They state that "action research merges research and praxis thus producing exceedingly relevant research findings" (Baskerville & Wood-Harper, 1998, p. 90). They also argue that "it is empirical, yet interpretive. It is experimental, yet multivariate. It is observational, yet interventionist" (Baskerville & Wood-Harper, 1996, p. 237).

More recently, the action research method has been applied in an IT Governance research project in a Latin American company. The researchers have successfully applied action research methods to investigate how organizational transition affects the implementation of IT Governance (Otto, 2010). Therefore, action research can also be seen as appropriate means to investigate issues of IT Governance in the domain of Emergency Management and identify conjoint solutions.

4.2.1.4 Qualitative Sources: Literature, Case Studies & Interviews

As mentioned the qualitative research part builds the foundation of the research project and therefore the data collection in this stage has to be thorough and sound. Emergency management and IT are complex and multi-disciplinary. Additionally, information on this specific topic is not very common. Hence, information has to come from numerous different sources to be meaningful. Since the qualitative content analysis is capable of incorporating different sources, the proposed research will make use of all of them. However, the primary sources for the qualitative content analysis are:

1. Two cases studies with large Emergency Management organizations, one of them Australian (Major Case 1) and the other German (Major Case 2). Additionally, four minor cases have been used to collect data.
2. Multiple narrative interviews with acting Emergency Management specialists from different organizations (state, NGO & private) to incorporate the different views in the models and methods
3. Observation of an multi-organizational pandemic drill
4. Internal documentation on conducted drills and disaster reviews.
5. Public secondary literature (e.g. disaster reports) with relation to this research

4.2.1.5 Validity and Credibility of Qualitative Research

Since qualitative research methods are mainly subjective and not totally objective it is harder to validate the quality of the data and the drawn conclusions. Patton (2002, p. 542) states that “judging quality requires criteria. Credibility flows from those judgements. Quality and credibility are connected in that judgements of quality constitute the foundation for perceptions of credibility”. Therefore, he developed five sets of criteria to ensure quality and credibility of qualitative research. These sets (see Figure 11) are to some degree overlapping and competing, therefore the researcher has to pick the right set of criteria for each underlying epistemology, research setting and research purpose (Patton, 2002):

EXHIBIT 9.1 Alternative Sets of Criteria for Judging the Quality and Credibility of Qualitative Inquiry

Traditional Scientific Research Criteria

- Objectivity of the inquirer (attempts to minimize bias)
- Validity of the data
- Systematic rigor of fieldwork procedures
- Triangulation (consistency of findings across methods and data sources)
- Reliability of codings and pattern analyses
- Correspondence of findings to reality
- Generalizability (external validity)
- Strength of evidence supporting causal hypotheses
- Contributions to theory

Social Construction and Constructivist Criteria

- Subjectivity acknowledged (discusses and takes into account biases)
- Trustworthiness
- Authenticity
- Triangulation (capturing and respecting multiple perspectives)
- Reflexivity
- Praxis
- Particularity (doing justice to the integrity of unique cases)
- Enhanced and deepened understanding (*Verstehen*)
- Contributions to dialogue

Artistic and Evocative Criteria

- Opens the world to us in some way
- Creativity
- Aesthetic quality
- Interpretive vitality
- Flows from self; embedded in lived experience

- Stimulating
- Provocative
- Connects with and moves the audience
- Voice distinct, expressive
- *Feels* "true" or "authentic" or "real"

Critical Change Criteria

- Critical perspective: Increases consciousness about injustices
- Identifies nature and sources of inequalities and injustices
- Represents the perspective of the less powerful
- Makes visible the ways in which those with more power exercise and benefit from power
- Engages those with less power respectfully and collaboratively
- Builds the capacity of those involved to take action
- Identifies potential change-making strategies
- Praxis
- Clear historical and values context
- Consequential validity

Evaluation Standards and Principles

- Utility
- Feasibility
- Propriety
- Accuracy (balance)
- Systematic inquiry
- Evaluator competence
- Integrity/honesty
- Respect for people (fairness)
- Responsibility to the general public welfare (taking into account diversity of interests and values)

Figure 11: Quality and Credibility Criteria (Patton, 2002, pp. 544-545)

Since Mayring's (2000) Qualitative Content Analysis approach is used throughout this research, the author also applied Mayring's 5 postulates / 13 pillars of qualitative quality to ensure validity and credibility of this research. These are shown in the following Figure 12.

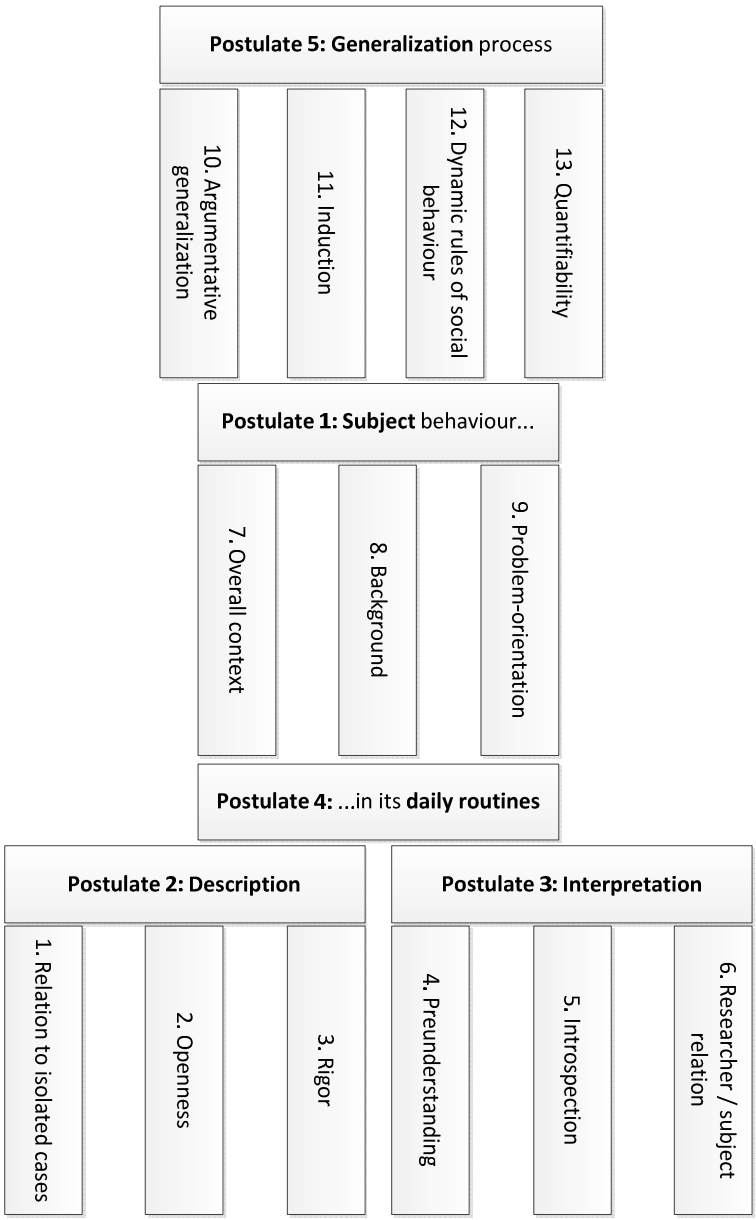


Figure 12: Mayring's (2002) 5 postulates / 13 pillars (adapted by author)

The five postulates represent the theoretical foundation of qualitative thinking and the 13 pillars can be seen as practical guidelines ensure the quality of qualitative research (Mayring, 2002):

1. Subject / Daily Routines: Research subjects are human subjects and have human behaviour. This human behaviour is researched best in a

daily environment or daily routine since it will reveal the complexity and relations of a subject and the environment.

   a. Overall context: Subject, environment and action have to be analysed as a whole
   b. Background: A subject's background is important to understand its behaviour, seniors might act differently than juniors
   c. Problem-orientation: Subject research should always focus on the research question

2. Description: Careful description of the research enables others to follow and reproduce the researcher's conclusions and interpretations.
   a. Relation to isolated cases: Descriptions should always start from isolated cases, to show find evidence for eventual generalizations and interpretations
   b. Openness: The research should be open to understand the research subject as a whole and describe it accordingly for later interpretation
   c. Rigor: Descriptions and the related tasks should be "controlled" to ensure a rigorous process and consistency
3. Interpretation: The research subject is never disclosed completely just by a detailed description. It also needs interpretation to deduce its full meaning.
   a. Preunderstanding: To draw conclusions and make interpretations the research need to have a certain degree of understanding of the research subject. This understanding will increase over time and enables the researcher to understand even more (see hermeneutic spiral chapter 4.2.1.1).
   b. Introspection: Since the research has a preunderstanding of the subject, interpretations are always biased to some degree, which is ok as long as the researcher is aware of this fact. This level of subjectivity is even necessary to discuss the findings and draw new conclusions.
   c. Researcher / subject relation: The relation between a research and the research subjects is dynamic and changes over time and from case to case. The researcher has to be aware that his

interaction with the subject can change the subject behaviour and therefore the results. Hence, a research need to estimate the impact of is actions in order to make conclusions.

4. Generalization: Generalizations are not generated automatically in qualitative research and are always subject to discussion. However, with a rigorous methodological approach generalizations can be justified by the underlying conclusions and interpretations.
    a. Argumentative generalization: All conclusions and interpretations are drawn from isolated cases. Hence, they are, by default, only valid for this isolated case in the first place. Since qualitative data cannot be used to proof its generalizability with a random sample, the researcher must find arguments for general statements drawn from these isolated cases (e.g. an additional expert evaluation)
    b. Induction: Instead of a deductive approach, the Qualitative Content Analysis utilizes an inductive approach to strengthen derived hypotheses and to draw generalized conclusions. Single observations are used to draw intermediate conclusions, which in return are used to find more supporting evidence for these conclusions in order to strengthen them or change them accordingly.
    c. Dynamic rules of social behaviour: Human behaviour does not follow fixed rules as in natural science, but humans do follow routines to a certain degree. When generalized conclusions are drawn from qualitative data it has to made clear that these conclusions are only valid under certain conditions and exceptions are possible.
    d. Quantifiability: Whenever possible and reasonable, qualitative conclusions should be supported with quantifiable data and triangulation methods.

Combining Patton's (2002) and Mayring's (2002) approaches will ensure reliability, creditability, and validity of the qualitative data and the drawn conclusions.

4.2.2 Modelling

The proposed research will make use of modelling techniques throughout the research process in order to develop a conceptual IT Governance approach for the domain of Emergency Management.

4.2.2.1 Conceptual (Reference) Models

According to Becker et al. (2007, p. 1) “reference models are generic conceptual models that formalize state-of-the-art knowledge of a certain domain”. However, it must be clear that a model can only show a frame of reality, not reality itself. Even though not completely realistic, it can help to overcome smaller, more manageable problems (Naumann, 2007; Rolf, 1998). Thus, a constant modelling process accompanied the previous mentioned research methods. Modelling relationships, and responsibilities with roles, functions and attributes will yield deeper insight and can close small gaps by providing new concepts (Heinrich & Sinz, 2002; Naumann, 2007).

The process of modelling will make specific problems and solutions more abstract and therefore can act as a reference and guideline for the researcher as well for the final users. Thus, reference models have much inherited from conceptual models.

Frank’s (2007, p. 119) definition of a conceptual model is “an abstraction that stresses the core terms or concepts which characterize an application domain, while neglecting technical aspects that are related to the implementation of corresponding software systems”.

Mylopoulos & Levesque (1980, p. 11) define conceptual models as “descriptions of a world enterprise/slice of reality which correspond directly and naturally to our own conceptualizations of the object of these descriptions“.

According to Frank (1999, p. 695) “it is widely accepted that conceptual models are a prerequisite for successfully planning and designing complex systems”. However, they require the participation and involvement of experts from the particular domain and can be seen as generic reference models.

Even though conceptual models and reference models are usually used to define the requirements for software development and customization of standard software, it is the researcher's belief that the same techniques are also useful to develop IT Management processes and methods. Consequently, a conceptual model will help the researcher to develop a realistic view on issues and improvements throughout the project. It will also give Emergency Management organizations a better understanding of their domain and gives them a 'reference' to which they can compare their own processes. This base-lining will help them to identify procedures which can be improved.

Besides reference models also metamodels can help to analyse and understand a research's objective, and ultimately develop new solutions by the abstraction and aggregation of real world elements and processes (Becker, Dreiling, & Ribbert, 2002, 2003). According to Karagiannis and Hoefferer (2006, p. 2) "metamodels most generally are defined as 'models of (other similar) models'". However, both (models and metamodels) refer to the same "real world object" but have a different degree of detail, which allows the observer to generalize conclusions derived from the subjacent tier. Figure 13 describes the different layers and their relation:

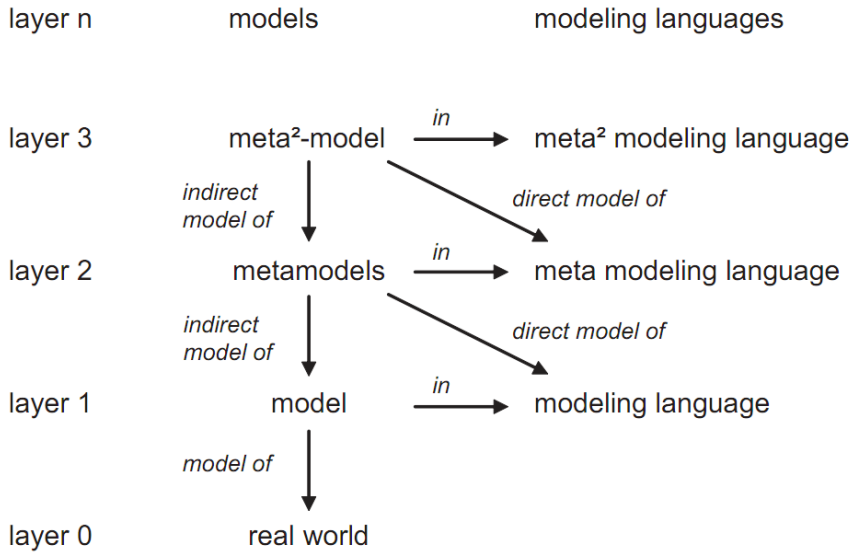


Figure 13: Real World, Models, & Metamodels as Layers (Karagiannis & Hoefferer, 2006, p. 3) adapted from (Strahringer, 1996)

Metamodels were only used on layer 2, layer 3-n were not seen as necessary for the research's objectives. This is oft referenced as "Macro-Level-Design"

and used to understand relevant “real life” concepts, which ensures that new instances of the models are structured in a way that all important aspects are considered.

Rolland (1993, p. 3) describes the abstraction as follows: “In IS development, a process model corresponds to the way of working prescribed by the methodology in use. It is similar to the concept of plan. The knowledge required to design such plans may be related to the third level of abstraction in process modelling and may take the form of a process meta-model”. See Figure 14.

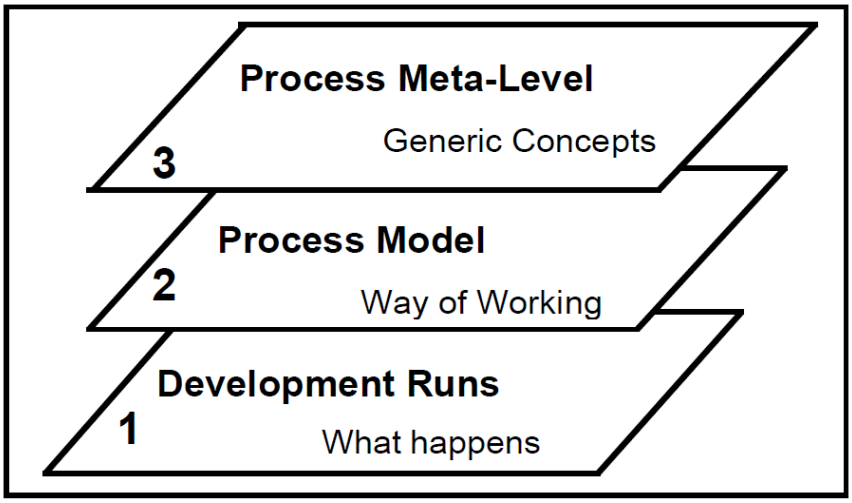


Figure 14: Abstraction Levels in Process Modelling (Rolland, 1993, p. 3)

This abstraction method has been used in two ways:

First, to create an understanding of the EM domain from the researched cases. In order to do this the real world (layer 0) was observed, and specific models were built for each case (layer 1). Then an abstract model of these models was created to identify the relevant and mutual processes or structures of the EM domain.

Second, the metamodeling approach was used to generalize existing IT Governance and IT Service Management frameworks in order to adapt them to the EM domain specific needs. However, such frameworks are already models (layer1), so it took only one step to build the metamodel. Moreover, the research was able to reuse some metamodel concepts of COBIT and ITIL from previous research (Goeken & Alter, 2008, 2009; Goeken, Alter, Milicevic, & Patas, 2009; Looso & Goeken, 2010).

4.2.2.2 Domain Specific Modelling / Engineering (DSM / DSE)

“Before processes and tools can be designed we must know the requirements. Before requirements can be expressed we must understand the domain” this adapted version of Bjorner’s (2010, p. 1) introduction to ‘Domain Engineering’ is simple, yet it reflects the basic idea behind this modelling approach.

From the literature and initial interviews surveys, it was learned that the researched domain has special rules and requirements compared to commercially driven enterprises. Things, which work effectively in a multi-national corporation, must not necessarily work in a local carpenter’s shop or during a highly uncertain emergency situation. Domain specific engineering (DSE) can be seen as a method, which could help to adapt existing frameworks, methods, and models towards the needs and requirements of specific domains. Consequently, a precise description of the domain has to be established first; then, from these descriptions, a researcher can “derive” the domain’s requirements; and from those requirements a researcher can model the appropriate processes and design the tools to support entities of this domain (Bjorner, 2010).

Considerations of domains in software development have always been there. Jackson wrote about domain specific development in 1975 already. In his view, the DSE approach helps to bridge the gap from a vague requirement, often expressed as assumptions, to a more detailed and implementable specification. A few other researchers, who explain the close association between domain knowledge and refinement of requirements, have followed it (Jackson, 1975; Zave & Jackson, 1997).

Even though most domain specific engineering approaches focus on software development, one can assume that it can also be used to alter existing IT Governance methods and ITSM frameworks towards the requirements of a specific domain.

Abstract processes and models are more accepted since more organizations will be able to relate to the model. Figure 15 shows a basic model, which was used as a starting point for this research. It does illustrate the general differences between the classical setting in industry and additional /

unpredictable influences in emergency situations. The model is on a very high-level, which gave the researcher a good guideline to understand the unique processes in the researched cases. It also enabled the researcher to design more detailed models for the participating organizations and identify issues and areas of improvements, which could be used for the final 'domain specific' reference model.

For this particular purpose, the researcher followed Naumann's (2007) approach of 'reference modelling for non-professional domains'. His approach is highly associated to NGO's, public organizations and non-for-profit organizations. Since Emergency Management is largely driven by such organizations this modelling approach, in combination with the basic principles described by Bjorner (2010), Jackson (1975) and Zave & Jackson (1997), is considered as most suitable for this research.

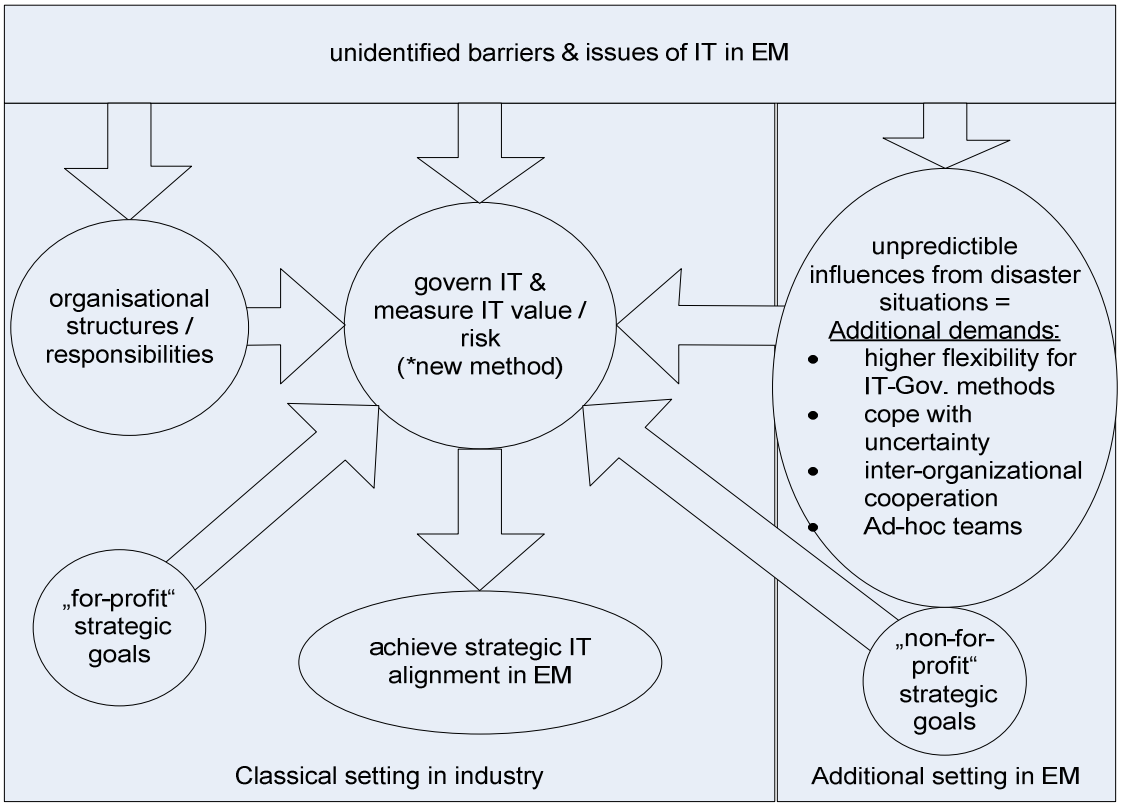


Figure 15: Starting model - high level

In order to follow Naumann's approach the researcher had to formulate a high level model (shown in Figure 15) of the EM domain. It reflects his preliminary understanding of the domain and the starting point for the hermeneutical analysis as explained in chapter 4.2.1.1. The figure shows how the researcher

initially understood the differences between the “classical setting in industry” (lower left square) and the “additional setting in EM” (lower right square) with regard to IT-Governance and IT value estimation tools (middle circle). The figure also shows how a “new method” is possibly influenced by yet “unidentified barriers & issues of IT in EM” (upper square) and how the major elements (surrounding circles from left and right) affect a domain specific reference model in order to “achieve strategic IT alignment in EM” (lower circle).

4.2.2.3 Evaluation of the Conceptual Models & Methods

The assessment of a conceptual reference model or framework is a challenging task. In addition to the problems known from the evaluation of conceptual models in general, reference models or frameworks claim general (re-) usability. They promise to provide appropriate descriptions of a whole domain and aim to deliver templates for ‘good practices’ of information systems and related organizational settings. Hence, they are known as descriptive, prescriptive and universal at the same time (Frank, 2007).

Even though this research does not focus on the design of information systems but rather their management, this definition can be reused for our purpose. Thus, Frank’s (2007) “multi perspective framework of evaluation” is used to evaluate the final model. He states that “an objective evaluation is hard to accomplish. Hence, the idea is to get closer to objectivity by fostering a more differentiated and balanced judgement” (Frank, 2007, p. 123). A general overview of his evaluation framework is shown in Figure 16.

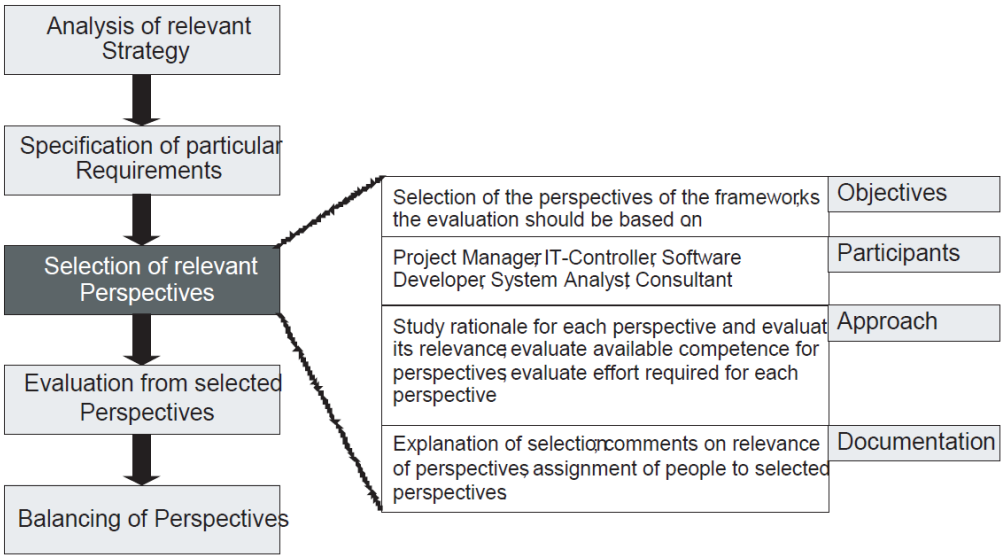


Figure 16: Model Evaluation Framework (Frank, 2007)

The framework suggests an evaluation based on the following perspectives:

- Economic perspective
- Deployment perspective
- Engineering perspective
- Epistemological perspective

All of these perspectives have numerous sub categories to assess the proposed model. However, some sub categories are not always applicable to all models.

Moreover, Frank (1999) states that even though frameworks for an evaluation are useful, and most categories can be assessed by the scientific methods used during the development, they are not sufficient. Only a discursive evaluation with a critical reflection from experts within the applicable domain can ensure the applicability and utility of conceptual models. Hence, the researcher decided to evaluate the models not only from an 'internal perspective' by using Frank's evaluation criteria, but also evaluate the models and methods from an 'external perspective' by experts in the field (see chapter 10.2 and Appendix H (Evaluation Survey & Results))

4.2.3 Quantitative Research

Quantitative research methods were originally developed in the natural sciences to study natural phenomena. Examples of quantitative methods are survey methods, laboratory experiments, formal methods (e.g. econometrics) and numerical methods such as mathematical modelling or statistics. In contrast to qualitative research, quantitative studies make use of numbers only. As a consequence, quantitative research claims to be unbiased and objective. However, the research methods cannot be applied directly applied to most social and cultural phenomena (Myers, 1997, 2008).

Even though Emergency Management is a complex area and qualitative methods are used as the primarily method, quantitative methods were used in later stages (see chapter 10.2.1) to validate the results. Since qualitative content analysis was used to collect data, quantitative methods were used to test and evaluate the final model. This triangulation approach was chosen to verify the conclusions drawn with a different research method and increase the validity and credibility of the results.

4.3 Discussing the Applied Research Design

This research has utilized mainly qualitative methods to identify areas of improvement and build a basis for the development of domain specific methods and models. In the final stage of the research, a quantitative approach was used to evaluate the effectiveness and applicability of these conceptual models and methods. The following diagram (Figure 17, p.91) and descriptions will explain the different research stages and activities.

1. Step one was a thorough literature review to build up a sound theoretical base. Predominantly focusing on related research and existing frameworks.
2. From findings of the literature, a semi-structured questionnaire with 22 questions was developed (see Appendix A (Interview Questionnaire)). The semi-structured approach was chosen to leave space for additional comments from interviewees, which were not covered by the questionnaire but might be useful for further investigations.

3. Initial interviews with a focus group were conducted to see if the research project is feasible and to identify the most common problems regarding IT Management and IT Governance.
4. All interviews were analysed by the means of NVIVO (QSR International, 2010) as the software tool and the Qualitative Content Analysis / Hermeneutics as the research method (Glaser & Strauss, 1967; Mayring, 2000, 2002; Myers, 1997, 2008). Due to ethical regulations, the interviews had to be anonymized. Hence, only important statements and answers from the interviewees have been transcribed (selective protocol). In case a statement or answer would reveal the interviewee or the participating organization the original statements was abstracted to a neutral level without altering its meaning. A large part of the interviews had been conducted in German. Thus, the important sections were translated into English.
5. Based on the findings from the focus group preliminary models, methods and processes have been developed and compared with existing frameworks and methods in order to identify space for improvements. These preliminary findings have built the basis for the coming in-depth interviews with the case study participants.
6. Conduct in-depth interviews with experts from the case studies and analyse internal documents to improve the models and methods.
7. Iterative cycle. Improve the preliminary model / methods (case study)
8. After a satisfying level of saturation was reached (no additional major improvement could be identified), final versions of the reference model and methods have been built.
9. Based on Frank's (2007) approach the models and methods were evaluated internally and externally. Thus, an "expert evaluation survey" has been developed using Likert-Scales (Likert, 1932) as a method of measurement for different attributes of the new reference model in order to identify where the conceptual reference model out- or underperforms existing methods and processes.
10. The final survey was sent to the International Association of Emergency Managers (IAEM) and the Association of Information Systems for Crisis Response and Management (ISCRAM). Participating organizations have

been excluded to minimize possible bias in the evaluation and test the general applicability of the models and methods. All assessors had access to the final models and methods, including some explanations via an animated PowerPoint presentation and the possibility to ask questions via email. The candidates compared the new concepts with the processes and methods of the organizations they have been working with. This identified under or over performing sections of the new model. Since all participants were contacted via official channels from Emergency Management associations, it was assured that all assessors had a strong expertise in the field and were capable to test and judge the final models and methods.

11. Since the Likert-Scale (Likert, 1932) of the survey could be transferred into numbers, the efficiency of the new model has been analysed with quantitative methods. The results gave an indication if the new model is universally applicable or not and which of the changes are superior or inferior to existing solutions.

Without combining different epistemological paradigms and research methods, it would have not been possible to tackle such a multi-disciplinary research project. Using only the interpretive approach and hermeneutics would have only helped in the first stage of the research where the main objective was to find out how Information Systems (IS) and Emergency Management (EM) go together. Even though it was paramount to understand the thinking and acting of EM staff in order to understand their perception of IS and its management, it was also crucial to apply the critical epistemological paradigm and identify weaknesses of existing frameworks, organizational structures and processes. Particularly Mayring's (2000) method of 'Qualitative Content Analysis' in combination with first organizational diagrams and process models turned out to be very helpful in these stages. It enabled the researcher to understand the issues of EM organizations with IS in general and IT Governance in particular. Using the constructive view helped the researcher to develop new concepts to overcome identified problems. The principles of action research helped to develop these new concepts since there was an iterative discussion during

the development and modelling phase with experts from the case studies. Finally, quantitative methods and a positivistic view have been used to evaluate the conceptual model and triangulate the results to add more rigor.

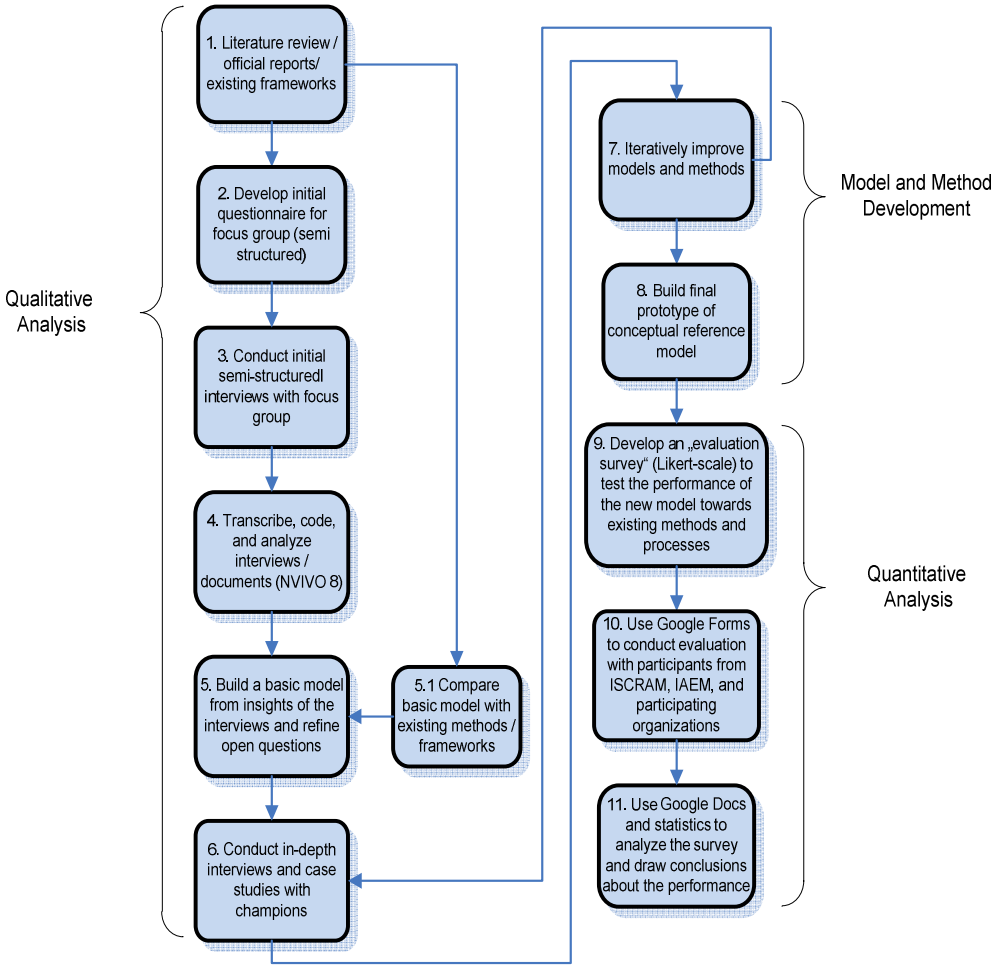


Figure 17: Research Method

PART III:
Data Collection & Analysis

5 Data Collection

As shown in the research methodology section of this thesis, primarily qualitative research methods have been used to collect and analyse the data. In total 32 interviews and approximately 45 hours of drill observations served as a basis for primary data. Numerous internal documents from the researched organizations (some of them shown in the appendix) and a few case studies from other researchers, who provided direct and relevant statements of their interviewees, have been used as a source of secondary data.

Since qualitative research is often seen with prejudice about its reliability and validity, a thorough description of the data collection and analysis process is essential for other researchers to follow and comprehend the findings and conclusions of this work. Mayring (2000) has developed quality principles, which guided this research methodology. One of his criteria highlights the importance of a thorough documentation since qualitative research methods are not as standardized as quantitative research (Mayring, 2002).

This chapter will therefore describe the data collection process for each set of interviews, survey, case studies, and observations. The analysed data, anonymized cases, process maps, and interview excerpts can be found in the appendix.

According to Arbnor & Bjerke (2009) two types of resources can be collected for a qualitative analysis: Primary data, which is totally new and collected by the researchers themselves, and secondary data, which was previously collected and published by other researchers or organizations.

The main information resource for this thesis is primary data. Arbnor & Bjerke (2009) have described three ways to collect primary data: direct observation, interviews, and experiments. This thesis utilizes only two of these primary data collection methods, namely interviews and observations. Both have been identified as the most promising ones. In addition, experiments have been considered at the beginning of this research; however, during the project initiation phase it was found that most organizations in the domain of Emergency Management are not very open to external research since they are

reluctant to disclose countermeasures. Therefore, it was hard for the researcher to earn the trust of EM organizations in order to conduct interviews and review their documents. As a result, only two major cases and four minor case studies could be researched. However, the data and input of these cases were quite rich and diverse. Therefore, the results and conclusions can still be considered as representative for this domain, particularly because intermediate results of this research have been regularly discussed with experts and researchers in the field.

Even though this thesis is primarily built upon primary data, it also uses secondary data to complement and verify findings whenever possible and necessary. Since officially published material on IT in EM organizations is scarce, secondary data used in this thesis consists mostly of documentation from the researched organizations (such as process maps, forms, meeting minutes, etc.).

Figure 18 shows a timeline of the data collection and analysis phases from the beginning to the end of the research project.

Figure 18: Research Timeline

5.1 Researchers Role

According to Fridriksson (2008) qualitative research is based on conversations with interviewees and interpretation of the collected data. Even though the researcher tried to keep an objective view, there is, without doubt, some bias and subjectivity included. Stake (1995, p. 135) states: “Qualitative case study is highly personal research. Persons studied are studied in depth. Researchers are encouraged to include their own personal perspective in the interpretation.

The way the case and the researcher interact is presumed unique and not necessarily reproducible for other cases and researchers. The quality and utility of the research is not based on its reproducibility but on whether or not the meanings generated by the researcher or the reader are valued. This personal valuing of the work is expected".

This chapter will illustrate the researcher's role and standpoint in order to show that the researcher was always aware of the fact that his results might have some subjectivity included and to help other researchers to understand the way of interpretation.

The first decision the researcher had to make was how active or passive he would be during the interviews and observations. Since the domain of Emergency Management was very new to the researcher, the working culture, habits, and attitudes of the interviewed people where unknown. Thus, a balanced approach was envisaged, which goes along with Kvale's (1996) statement that it is important to become part of the subjects domain and find a good balance between debating and listening. A too passive behaviour might not bring the best results since the implicit knowledge of an interviewee might not be revealed when an important point is not actively discussed, or the researcher gets lost in the subjects domain specific terminology and is therefore unable to follow the subject's explanations. As a result, this would influence the study and yield incorrect findings or lead to wrong conclusions. On the other hand a too active approach can force the interviewee to make statements he (or she) thinks the researcher wants to hear, or it will lead to some kind of action research in which the researcher himself would become part of a the study (Costello, 2003; Kvale, 1996).

The first hurdle of this research project was getting access to stakeholders and relevant documentation in the EM domain. Most of the EM organizations and critical infrastructure providers (CIP) have sensitive data, which could be misused in wrong hands (e.g., evacuation plans in case of a terror threat). Thus, it was not easy to earn the trust of these organizations since the researcher came from an external organization. For that reason, the researcher had to establish his own personal network within this domain. Starting from his own circle of friends and colleagues to becoming an active member of IAEM

(International Association of Emergency Managers) and ISCRAM (Information Systems for Crisis Response and Management). This network enabled the researcher to establish personal connections with stakeholders in EM organizations. During this process, the researcher became familiar with the domain specific terminology, which turned out to be a cornerstone for his acceptance as “full member” of this domain. One could see this as a problem and argue that such personal relations and involvement in the domain will cause massive subjectivity and it might be true to a certain extent. However, as stated above “subjectivity” is always involved in qualitative research and true objectivity a myth. The reader should see these relations as an enabler to access the research domain since the researcher tried to take a distance stance whenever this was possible in order to maintain as much “objectivity” as possible.

At the beginning of each interview the researcher made clear that, he is an academic researching the IT issues in EM organizations. During the observations and interviews, the researcher was asked for his own opinion as an academic from time to time. While trying to keep some distance only theoretic and uncritical answers were provided instead of personal and controversial thoughts. With this approach, it was tried to keep every conversation on an objective level and eliminate as much subjectivity as possible. However, the researcher was aware that his answer was still somewhat “subjective” and could have influenced the interviewee’s in his/her following answers. Whenever the researcher had the feeling that the interviewee’s answers were “untrue” or “politically correct” the researchers made notes and treated the data accordingly in the later analysis. Fortunately, this only happened twice during the interviews and the topic was changed immediately so the rest of the interview was not affected. As a general rule the researcher kept silent during observations and during interviews unless he was asked something or had problems to follow the process. The researcher did not break into someone’s explanations as long as he/she was not drifting apart too much or further explanation was needed to understand the interviewee’s point of view completely. This way it was tried to keep interruptions and interactions at a minimum.

The fact that the interviewer and observer identified himself as an external academic could have influenced the answers and behaviour of some of the participants. In which way this had an influence is not entirely clear, however, it can be confirmed that nobody had an issue with the attendance of the researcher or at least expressed his concerns about his attendance. The researcher believes that his academic status had, if any, only minor impact on the answers (e.g. in the way of framing a sentence, but not altering its meaning). Thus, this possible influence factor was deliberately neglected in the research data.

As shown in the previous chapter there are three major research stages, first data collection, second the modelling/design phase, and third the evaluation of the conceptual model. Certainly, the first stage was the longest and the researcher spend quite some time in a rather passive role as described above. However, the second stage (modelling) was shorter but forced the researcher into a more active role. Based on the data of the first stage the researcher had developed preliminary models and discussed them iteratively with some of the participants as well as with other researchers and experts in the field. In this stage the researcher utilized an action research approach in order to have a discourse about his intermediate results. The epistemological assumptions in this phase were based on critical and constructive views.

In this stage the researcher took a bit of an aggressive but yet respectful stance. In some cases the researcher went into controversial discussions about how EM organizations are governing their IT (if at all) and how they possibly should govern it. However, these discussions happened on a very professional level and the researcher never had the feeling that participants felt personally attacked. It was rather a very fruitful and constructive collaboration, which always ended with a mutual agreement about further changes for the intermediate models and methods. Most changes had to be made in the “as-is” models since the participants where familiar with the processes in their company, less changes had to be made in the generic models and methods since they are designed on a more abstract level. This was an indication for the researcher that different organizations can relate to these generic concepts. The modelling stage ended at the time when the participants had no more

requests for major changes in the conceptual models. At the end of the modelling phase, some participants still requested smaller changes, but these were seen as rather specific and only relevant for the particular organization. Hence, they were not considered in the final conceptual model since it should represent a generic approach to which other EM organizations should be able to relate to.

The final evaluation process was rather anonymous to reduce the eventual bias in the evaluation. Therefore, there was almost no interaction between the researcher and the participants but the request to participate in the evaluation, which was done via email and internal newsletters of IAEM and ISCRAM. The researcher provided the participants access to an animated PowerPoint presentation explaining the research and showing the final conceptual models and methods. The presentation was based on 63 slides with numerous animations and textboxes. In addition, the participants were able to download sheets containing information about the adapted processes. It was tried to provide enough information for those who had not been involved in this research so far, but since it was anticipated that some participants might have additional questions or comments, which were not covered by the provided information or the evaluation survey, it was offered to correspond via email. However, only one participant wanted to clarify some details.

In summary it can be said, that the researcher tried to get as much primary data as possible about the EM domain from the interviews and the observation. This was only possible as an accepted member, not as an invisible “fly on the wall”. The close relations were necessary to understand the study object and also to understand the different thinking patterns of EM organizations and understand the complex context. Nevertheless, whenever possible he tried to take a passive stance. Thus, the researcher’s views are certainly subjective, but he tried to keep as much objectivity as possible by using a rigorous research methodology and a transparent documentation of the research steps (Arbnor & Bjerke, 2009; Mayring, 2000, 2002).

5.2 Participants

According to Gorman, Clayton, Shep, & Clayton (2005) it is important to interview different stakeholders within and across organizations to understand complex situations and circumstances. This is particularly true for IT Governance related research since input from both sides – the business and the IT perspective – is needed (Weill & Broadbent, 1998; Weill & Ross, 2004). This allows the researcher to analyse different views and find correlations and repeating patterns from which generalized assumptions can be derived. However, it is also important that the researcher select interview partners, who can give significant input, demonstrate strong knowledge about the researched area, and have independent thinking patterns. Additionally, the participants should not be too shy to defend their point of view and share their ideas though these might be controversially discussed amongst their colleagues. This ensures that the information retrieved from the interviews is adequate and valid. Hence, only senior IT and EM personnel as well as researchers and experts in the domain were interviewed and surveyed for this research project.

All organizations or individual employees of the researched EM organizations have shown interest in the project, were willing to support it with access to documents and procedures, as well as their personal input. Thus, their answers and comments were seen as valid and useful for this research.

A positive factor was that this project was a constellation of different organizations and actors that all had their own experiences that would contribute to new insights or joint understanding. All of those involved, i.e. the organizations' representatives, held management positions, or key roles. These circumstances were seen as a good possibility to discuss issues in a way that would certainly differ if all the interviewees had been volunteers and only occasionally involved in emergencies.

After connections to the participating organizations had been established and the researcher was accepted as a "full member" of the domain, it was relatively easy to get access to the participants. The researcher always felt welcome and could either call them by phone, communicate via email, or visit the organization or participants in their office after an appointment was made.

Due to ethical regulations and confidential data provided by some of the participating organizations, the names of the organizations and interviewees had to be anonymized. However, they are briefly described below to give the reader an impression of the validity and quality of the collected data.

- Major Case 1 (State government / AUS)
- Major Case 2 (Large municipality & fire and rescue services/ GER)
- Minor Case 1 (Flight Rescue / GER)
- Minor Case 2 (Local Red Cross chapter / GER)
- Minor Case 3 (CIP/ GER)
- Minor Case 4 (Chemical Plant / GER)

In addition to these cases, interviews and surveys with members of the following organizations have been conducted

- ISCRAM (Information Systems in Crisis Response and Management) Research Community (worldwide)
- IAEM (International Association of Emergency Managers) Research Community (worldwide)

However, due to the limited time frame, resources, and the obvious diversity of participating institutions two participating organizations have been identified, which are comparable and complex enough to become the major case studies and assist during the development phase of the project. Both organizations are governmental institutions and responsible for Emergency Management either on large municipal or state level.

The intensity of research and conducted interviews varied between these organizations due to accessibility and involvement of the stakeholders. Particularly Major Case 2 has delivered the riches set of data closely followed by Major Case 1. However, all of the interviews are relevant in order to develop generalized models and methods. Particularly members of ISCRAM and IAEM were most valuable for the final testing phase since they are distributed over different Emergency Management organizations worldwide. Hence, the results can be seen as generally applicable, even though the input to this research came only from a small subset of these organisations.

5.3 Interviews

This research is based on empirical material gathered during almost two years. The data collection started in January 2009 with a literature review and secondary data. First unstructured interviews with EM personnel were conducted in March 2009 and ended in November 2010 with a set of semi-structured interviews. From December 2010 to August 2011 the framework was iteratively developed, frequently discussing intermediate results with other experts in the field. The final framework was evaluated by a survey in October 2011.

One question that had to be answered during the data collection process was “when to stop”? In contrast to some quantitative methods, there is no maximum or minimum since the hermeneutic spiral is an iterative process. Thus, interviews were conducted until the researcher felt that a satisfactory level of saturation was reached and additional interviewees would not reveal other meaningful insights. Hence, it was an abductive analytical approach that aimed for a good effort/benefit ratio without missing important information.

The main interest of this research lies within the process perspective, the organizational structures, and the IT strategy of the individual organization as well as the interaction of temporary teams in an inter-organizational setting (cp. Achtenhagen, Melin, Müllern, & Ericson, 2003). The aim was to find weak process structures and to identify methods, which will help the organizations to tackle these problems. Thus, this thesis should contribute to a better understanding and acceptance of IT opportunities in EM organizations and lead to a better alignment of IT investments.

In the beginning of this project, the researcher had only a rough understanding of what he was expecting and what he was looking for since literature about this topic is scarce. However, during the empirical study and the hermeneutical approach the vision became clearer. Therefore, the first stage of interviews had an open character with the aim to generate narratives from the interviewees about the domain. These rather casual meetings enabled the researcher to establish his own personal network with the domain of EM, which gave the researcher the opportunity to get access to more information resources. The

second set of interviews was more standardized, so a semi structured interview guideline was used during these interviews. The semi structured set of interviews was complemented by two major case studies, four minor case studies, and an observation of a pandemic drill. An open and semi-structured research approach, as applied in this project, has been identified as a fruitful data collection method in complex environments (S. E. Chase, 2003; Schütze, 1987).

32 interviews have been conducted in total. Interviewees of the two major cases have been interviewed up to three times. Each interview lasted between 30 minutes and almost three hours, even though the envisaged time was only 60 minutes. Some of the participants were happy to discuss the topic in depth, gave detailed examples, or started to show their emergency response centres while explaining the different functions. As a result, the timeframe was extended to several hours and the semi-structured interview brought more information than anticipated. Other participants had a very limited timeframe, so only the most important questions could be answered, and other questions had to be skipped. Even though this was unfortunate, it was not a big issue in terms of data analysis since the leading research method, Qualitative Content Analysis, is able to cope with such variations (Mayring, 2000, 2002).

During the first and second set of interviews, only one participant was interviewed per session. In the major case studies and the observations it could have happened that a group discussion was started since there were two or more participants involved. This was not intended but was highly appreciated by the researcher since these discussions were authentic and revealed valuable insights. Since the participants of Major Case 2 were highly involved in this research, the researcher was asked to give sporadic and brief recaps to the participants as a group, so the organization “can learn” from the findings. One could argue that this action could have influenced the participants’ perception and therefore altered the following answers. However, as said in the previous section, only issues have been discussed which were raised by one or more of the participants at first. The intention behind this was not only to strengthen the level of trust with this organization and create a win-win situation, it was also done from a scientific perspective. The debriefing gave the participants the

opportunity to discuss the issues together, which gave the researcher valuable information on the credibility of the single answers and get richer information.

Most of the interviews had been recorded to transcribe relevant passages afterwards; in some cases this was not possible so only notes were taken. However, due to ethical regulations the answers had to be anonymized immediately for privacy issues. Since this is not a research in social science but rather an IT Management project, the researcher neglected pronunciation and body language unless it was important to stress particular issues. The research is focused on content and context and does not primarily intend to analyse the participants behaviour or reactions. Thus, answers and comments have been altered and sometimes summarized towards a better readability. Noticeable and important citations were only changed to a minimum and when needed. These alterations are not seen as influential during the analysis phase and can therefore be neglected. Mayring (2000, 2002) has mentioned this transcription technique as “summarized content analysis” and “selective protocol”, an efficient and often sufficient technique in domains with a background in natural science. The summarization approach goes hand in hand with University’s ethical code to anonymize the interviews. Thus, nobody should be able to identify an interviewee by typical or personal speech patterns.

Some of the interviews were conducted in German since this was the participants’ mother tongue and thus the answers and comments had to be translated during the transcription process. Conducting the interviews in German ensured that all questions were understood completely and answers could be given without language barriers. Since the researcher himself is a German native speaker, this was more of an advantage than an issue for this research project. The researcher himself made all translations and relevant transcriptions so the meaning was not altered unintentionally.

5.3.1 Unstructured interviews (Focus Group)

Early in the beginning of this research project it became clear that interviews with a focus group were needed to get access to the domain and ensure that the identified research gap is not only existing in the literature but also of practical relevance to EM organizations. Following the defined research

methodology, the first interviews were rather open and loosely structured. It was the intent to understand the domain of Emergency Management and their primary Information Technology (IT) and Information Systems (IS) issues.

Following objectives had priority in this phase of the project:

- Get general information about IT/IS utilization and IT/IS management methods in EM
- Refine the research methods and questions based on the collected information and set appropriate limitations
- Get access to the domain and establish connections to stakeholders
- Become aware of the total scope of activities and get a feeling for the complexity of this domain.

Interview partners were selected 'randomly', the only constraint was they had to work with an EM organization. Size and complexity of the companies were neglected at this stage and it did not matter if they were private or public organizations. Thus, the researcher started with local fire brigades, Red Cross chapters, local government, and a critical infrastructure provider in Germany. In this stage, 14 organizations were involved. Since the researcher had not had access to mid-level or upper level management, the interviewees were usually from the EM operations. Even though the initially collected information was not very rich, it gave the researcher a good understanding on the operational level. Additionally, the local representatives have opened the door to higher management in these organizations. Since this was a relatively unstructured phase of the research, it took longer than anticipated (March 2009 – November 2009).

5.3.2 Semi-Structured Interviews

The interviews with the focus group were followed by a phase of semi-structured interviews. According to Dunn (2000) semi-structured interviews are seen as the best technique to gain information from different viewpoints. The questionnaire focused on the general applicability of IT Governance methods an IT Management issues. The semi-structured interviews were conducted in nine participating organizations. Two of them were large municipalities and

state agencies (>250 employees), two were large critical infrastructure providers (>250 employees), three were medium sized first-responders and related EM organizations (50 – 250 employees), and two were smaller organizations (<50 employees) working in the EM field. The general questions for these semi-structured interviews were:

- What are the primary IT related issues in EM organizations
- What are the most used IT Governance frameworks and methods
- What are the most important issues and benefits of existing IT Governance frameworks and methods in this domain
- What are the major differences from commercially driven organizations
- Who is making IT related decisions
- What does the IT infrastructure look like
- What does the IT Governance process / IT Management process look like
- How do EM organization evaluate and prioritize IT investments

This phase of the project was targeted towards stakeholders in EM operations and IT units from participating organizations. However, the number of participants and suitable interview partners, which had the right expertise, was very limited. Therefore, only one questionnaire for both – IT and EM staff – was used. Consequently, some of the questions were too specific and not every person was able answer them completely.

The close connection between the researcher and the interviewee was an excellent basis to get a detailed view on important issues and helped the researcher to expand the structure of the interview on-site if new and interesting topics came up, or if certain statements needed more explanation. According to Cavana, Delahaye & Sekan (2001) and Tashakkori & Teddlie (1998) such flexibility enables the researcher to control the interview and get the most important information without losing the red line.

5.3.2.1 Development of the Semi-Structured Questionnaire

The interview questions (Appendix A (Interview Questionnaire)) were separated into four main sections:

- Demographic data
- Questions to the organization
- Questions to operational processes
- Questions to IT alignment

They questions were ordered in an increasing difficulty starting from easier questions to questions that are more detailed. Purpose of this separation and order was to establish a connection between the interviewee and the interviewer (Dunn, 2000).

5.3.2.2 Conducting Interviews

The questions were handed out to the interviewees before the actual interview, either in person or via email. Thus, they had the time to prepare themselves and did not feel insecure during the interview. The interviews were conducted in person and were recorded whenever necessary and possible to identify the relevant answers in a later review of the interview. All interviews were conducted in the mother tongue of the interviewees to ensure there were no misunderstandings, and took place in a familiar environment of the interviewee - usually their workplace.

At the beginning of the interview, the interviewees were given a brief explanation on the background of the research and the objectives of the study. They were also informed that the session would be recorded, and that only anonymized parts of the interview will be used for data analysis and publication. The interviewees were asked to sign consent forms in order to document this agreement. This practice ensured compliance with University's ethical research guidelines and gave the interviewees sufficient information on their right to break up the interview at any time.

The questions were usually asked according to the original order in the interview schedule. However, in some instances the interviewees tended to answer questions that had yet to be asked while answering other questions. Hence, the researcher had to adjust the order of the questions to ensure that the most important questions had been answered by the interviewees.

In some cases, the interviews became very dynamic and the interviewee revealed insights, which were not covered in the questionnaire. This was mostly very interesting since the collected data became even richer. In other cases, the interviewees were not able to answer all questions or had not enough time to answer all questions. In this case, the researcher tried to rearrange the interview questions to get as much input as possible.

5.4 Case Studies

Case studies are excellent research methods if only little is known about a certain area since they help the researcher to get a deeper understanding of the complex processes and relations within a domain or organization. Cases enable a researcher to analyse procedures and habits in a complete context, which is necessary for interpretations and conclusions. To analyse the often multi-disciplinary cases, a researcher can use different qualitative methods, such as interviews, observation, and secondary sources (e.g., internal documents), as well as quantitative methods such as statistical data (e.g., trend analysis). Hence, case studies can be positivistic, interpretive and/or critical, depending on the underlying philosophical assumptions (Eisenhardt, 1989; Fridriksson, 2008; Ghauri & Gronhaug, 2005; Myers, 2008; Yin, 2009).

As already stated in the introduction, research about IT Governance in the EM domain is very scarce. In addition, the processes and organizational structures of this domain are very complex and multi-disciplinary. Hence, cases studies were an ideal method to derive the right information in order to make conclusions and develop new methods and conceptual models. The primary intent of the case studies was to get an understanding of the complex processes in EM organizations in order to analyse their IT Governance maturity and capability. Examples of as-is processes and analysed documents can be found in the Appendix.

As with the previous interviews, all names of the participants and organizations had to be anonymized due to University's ethical guidelines. In some cases the organizations demanded and additional non-disclosure agreement to ensure that no sensitive data will be given to a third party by the researcher. This was

done because some information was seen as critical if published (e.g. counter-terrorism processes). Therefore, such information was used in an abstracted version in this thesis. Even though this will limit the transparency of the research results to some degree, it should not limit the validity or integrity of this research project since only the relevant processes, organizational structures, barriers, and opportunities are of interest, not the names of participating organizations or persons. Whenever necessary, the expertise, function, or background of an interviewee or an organization was documented to ensure validity and integrity of their statements.

5.5 Drill Observation

Observation is a standard method in field-research and particularly useful for research objectives, which need a very close and personal involvement in order to be analysed. Moreover, some research objectives can only be accessed by an observation. Therefore, it is used to research participants and their actions in the context of a real life situation, or in case of an exercise, in a near real-life situation. The observation of a pandemic drill was used to collect data about the environment, processes, and people. Thus, an observation can generate a deeper understanding than interviews or surveys about a particular research area, because it provides much more detail and context. It can also enable the researcher to unveil issues and problems, which were yet unknown or unrealized by participants themselves, or issues and problems, which are deliberately not discussed or concealed due to personal interest. (Ghauri & Gronhaug, 2005; Mayring, 2000, 2002; Myers, 1997, 2008; Patton, 2002).

These characteristics and features of an observation were the reason to use it in this research project as a data source. The observation of a multi-organizational emergency drill (pandemic influenza / swine-flu), which was conducted over several month gave the researcher insight in the use and application of information technology, information systems, information management, decision making, and the issues attached to it. Without the observation of a drill exercise, the researcher would have not been able to see how IT is used during a near real-life emergency situation. Main goal of the observation was to capture realistic processes of multiple EM organization from

a personal view and not only relying on the participants' own interpretation of how well they have their IT processes structured or how well they have implemented IT or IT enabled services in their routines.

The observation was done with maximum distance to the participants, the researcher did not involve himself directly in the EM process, nor did he comment the actions during the drill. The only interruptions caused by the researcher were questions if something was not clear. To reduce the amount and impact of interruption a liaison was assigned to the researcher by the leading organization. This liaison either answered the questions himself or established the right contact to other organizations at a convenient time so they were able to answer the questions themselves.

The observation was conducted using a semi-structured approach. This approach was chosen to stick to a red line but also leave enough space to investigate aspects, which have not been considered before the start of the drill observation (Fridriksson, 2008; Mayring, 2000, 2002). The following questions were used as a guideline throughout the observation process:

- What kind of information technologies (IT) are used during the drill?
- Are there technologies, which are available but not used by the EM personnel?
- Are there technologies missing, which could help EM personnel?
- Is IT implemented ad-hoc?
- Did all technologies function as they should?
- Are IT and IT Services monitored and managed proactively?
- Is their IT integrated, or are there IT islands?
- How is information forwarded?
- Was all information received?
- How is information processed?
- How are IT related decisions made?
- Is there a shift in the responsibility, accountability, consulted, and informed (RACI) matrix
- Does the organizational structure change?

During the observation, only pen and paper were used to make notes. This seemed to be the most appropriate way since the drill took place in several offices distributed over multiple buildings in the initial phase, and in the final phase in a large three story emergency operation centre (EOC) with several offices. Hence, the researcher was forced to change locations quite regularly to analyse the complete situation. Therefore, a Laptop was considered as too inflexible and disturbing for the participants (e.g. keyboard noise, power cables lying around, etc.). Notes about conversations and actions were taken based on relevance to the leading research questions and immediately commented with personal impressions by the researcher.

In a kick-off meeting all participants were informed by the leading organization that a researcher will observe the drill, but all retrieved data will not be disclosed until it is anonymized to a satisfactory degree. This was not only done due to University's ethical regulations but also to ensure that all participants were relaxed and acted as usual during the drill. Thus, all participants were asked if there would be any reservations against the presence of an external observer, which was not the case. All participants welcomed the presence of the researcher and assured their assistance. Additionally, every participant was told that he or she would have the right to dismiss the researcher temporarily if very sensitive information was discussed during the drill exercise. This happened only once during the whole exercise.

5.6 Evaluation Survey

The survey for the 'expert evaluation' was designed using 'Google Forms' and 'Google Docs' since they were freely available to the researcher and provided sufficient analytical features. Because possible participants were spread over the globe, this turned out to be the most suitable media concerning development, acceptance, and distribution. Since the researcher did not know the participants, anonymity was given and the survey complied with University's ethical code.

The survey questionnaire was used as the main data-gathering instrument for the 'evaluation phase' (see Appendix H (Evaluation Survey & Results)). The

questionnaire was divided into two main parts, an initial demographic section, and a main survey section.

The participants had approximately four weeks' time to read the information provided and to complete the survey. This ensured that they had enough time to assess the conceptual models and methods against their existing methods and procedures. By the means of 'Google Analytics' the researcher was able to monitor statistics about "downloads" and "click statistics" for the survey and the associated information. As expected, the access slowed down towards the end of the four weeks, which was an indication that no more participants are willing to take part in the survey. The data collection for this final phase started on 9th October 2011 and closed on 8th November 2011.

At the end of the data collection phase, all surveys were tested for validity and completeness. To analyse and evaluate the collected data simple statistical methods were used to identify the performance of the new methods and models. Details about this phase can be found in the appendix.

6 Analysing the Qualitative Data

The following sections will describe how the collected data was analysed. As mentioned above the qualitative part consisted of 32 interviews, 6 case studies and the observation of a pandemic drill.

6.1 Interviews

A total of 32 semi-structured interviews have been conducted in nine organizations of which six became also the case studies. 20 of the interviews were done face-to-face, in most cases the researcher was able to use a recording device to leave enough time to analyse the answers and transcribe important sections after the interview. However, in some cases the recording device was either not allowed or could not be used due to technical problems. In this case the researcher took notes and tried to transcribe important statements immediately during or after an interview. The 12 follow up interviews, in which the researcher asked for more information about previous explanations of an interviewee or provided documentation, were conducted by phone and notes were also taken on paper.

As described above the interview phase was split into two phases. The first one was unstructured, and the second semi-structured. The first six interviews were conducted unstructured in order to build an understanding of the domain. From the beginning of the research until the end of the data collection and analysis the researcher utilized NVIVO (QSR International, 2010) as the software to conduct the Qualitative Content Analysis (QCA) (Mayring, 2000).

6.1.1 Coding Schemes, Nodes, and Sources

NVIVO and QCA are based on structures and coding schemes. The coding scheme uses “Nodes” and “Sources” as the basic entities of this method. Nodes reflect important “topics” or “ideas”, which can be found in the sources in recurring patterns. Such recurring patterns could be for example “IT Security Issues” and reflect statements of interviewees regarding these issues.

Sources can be transcriptions from interviews, documents, video files, pictures, or any other source of information that can be useful to analyse a research objectives. Either the whole source or parts of it can be linked to nodes for further analysis. For example, a complete source can be linked to a particular cases study (e.g. case 1) or marked as an interview with a particular group of people (e.g. IT staff). Such a categorization can help the researcher to draw conclusions (e.g. majority of IT staff mentions “A” whereas EM staff mentions “B”).

The structure can reflect correlations between these nodes. Parent nodes can be used to summarize nodes with a similar topic or idea. Child nodes can be used to refine such ideas and retrieve a better or more detailed understanding of the research’s objective.

Following the hermeneutical approach, the coding of sources, drawing conclusions, conducting interviews, and re-coding the schema is an iterative process. The first coding scheme was rather simple since the researcher had only basic knowledge about this domain. Hence, this initial scheme went through a couple of iterative cycles. Nodes were created, merged, and restructured until the final coding scheme was reached as shown in Figure 19.

The coding scheme changed over the time and the interviews revealed more than shown in this coding scheme, but these nodes were seen as the most relevant for this research’s objective in the final stage of the data analysis. Certainly, another research would have found different nodes important or would have rearranged or renamed the nodes. As mentioned prior, qualitative research is highly subjective. The coding scheme consists of five main categories:

- IT Framework issues
- IT Governance Issues
- IT Service Management Issues
- Other IT Issues
- Resources

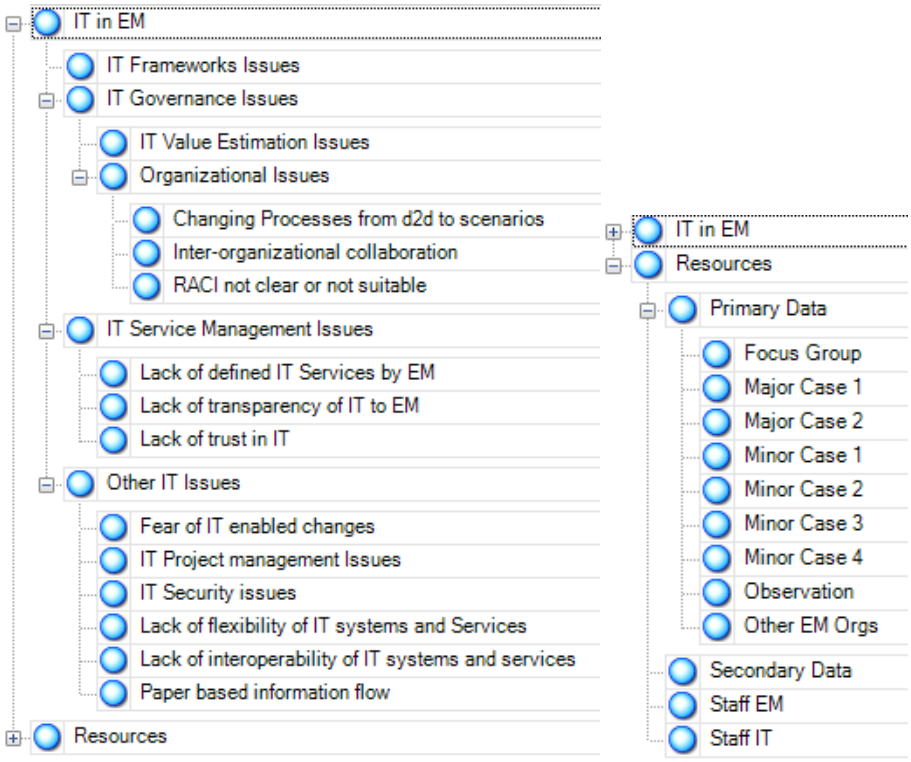


Figure 19: Coding Scheme in NVIVO

"IT Framework issues" contain references, which relate to problems with existing IT Governance of ITSM Frameworks. In the early coding schemes, it was tried to identify issues of particular frameworks so this section had sub-categories named ITIL, COBIT, Val-IT, etc. but it turned out that interviews were too short and not the suitable approach to identify issues with particular frameworks. This was later done by the action research approach. However, these nodes revealed general issues of these frameworks, which guided the action research and the discussions in this phase. The general issues were:

- Complexity and extent of existing frameworks
- Inflexibility of some processes
- No EM specific terminology
- No relation to EM operation

"IT Governance Issues" were linked with references to "IT Value Estimation Issues" and "Organizational issues". These categories were seen from a strategic perspective and therefore separated from IT Service Management Issues, which was seen as more operational. In combination with the process analysis of the major and minor cases these nodes revealed the main problems

of the researched EM organizations with regard to organizational structures and IT value estimation & prioritization methods. It also indicated in which way existing structures and methods need to be altered and adapted in order to become more useful for EM organizations.

The category “IT Service Management Issues” was used to identify operational issues in EM organization. In combination with the identified “IT Framework Issues” and the discussions with EM personnel about “AS-IS” and “TO-BE” procedures they were used to develop domain specific ITSM processes.

The last IT focused node “Other IT Issues” was used to collect the rest of the relevant references, such as “IT Security Issues”. These nodes were mostly categories, which neither fit into the strategic or operational category but influenced both to certain degree.

The last category “Sources” was used to find trends amongst certain groups of interviewees.

6.1.2 Coding Sources

As described in the previous chapter “Data Collection”, important sections of the interviews have been transcribed into NVIVO for further analysis.

NVIVO allows the researcher to mark particular interesting sections of the transcribed interview and link this marked section to one or multiple nodes, which seem to be relevant. As with the coding scheme, this is a very subjective task and most likely different researchers would mark and link different sections to different nodes.

Figure 20 shows an example how sources were coded in NVIVO.

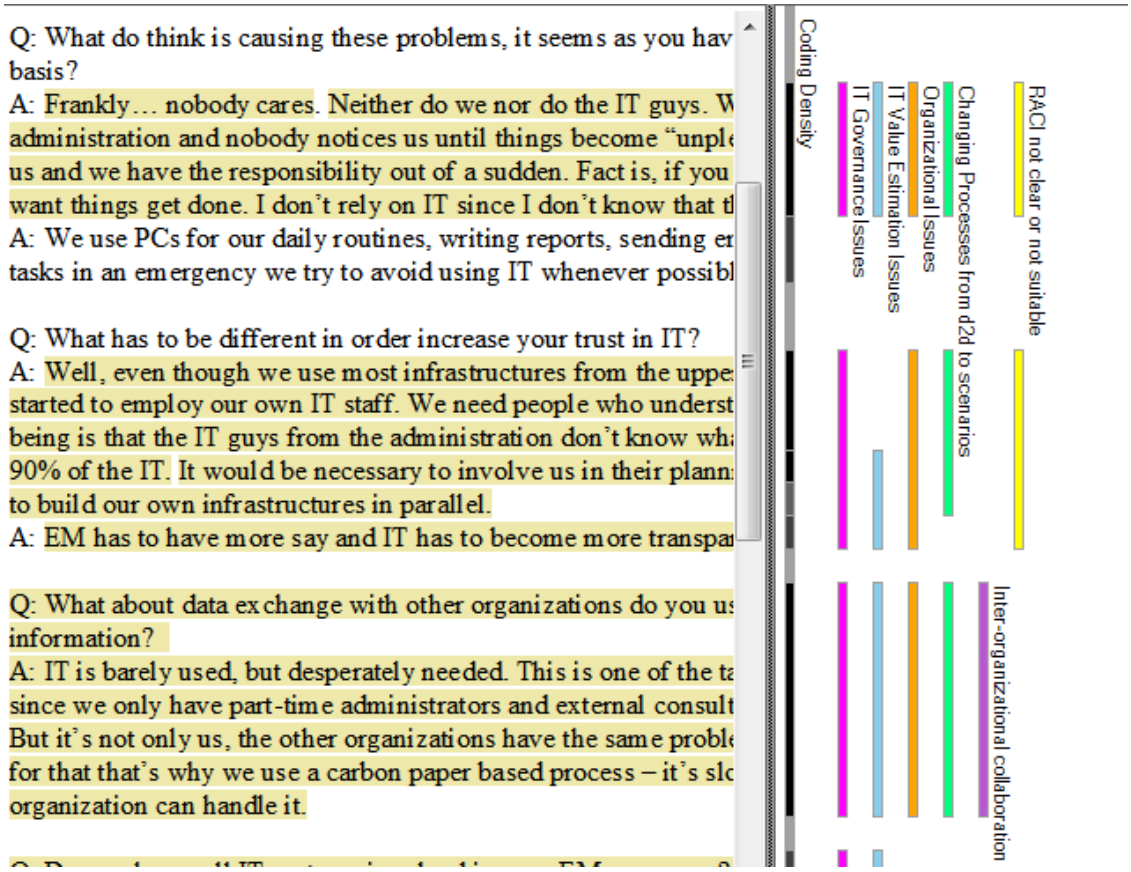


Figure 20: Coding sources

On the left side of the screen shot one can see the transcribed content and the marked sections. Immediately to the right the researcher can see the coding density. This helped the researcher to identify important sections with a lot of information, or sections, which might need a revision. The coding density in this example is quite high (black), which can be explained by the "summarized content analysis" and "selective protocol" as describe in the previous section "Data Collection" (see also Mayring, 2000; Mayring, 2002). If the interviews would have been transcribed completely the coding density would have been lower since some sections would not have been relevant.

The coded nodes can be seen as coloured stripes in the outer right of this figure. Different nodes use different colours to see which section of the text relates to particular nodes. Due to this sectional coding the researcher was able to summarize all statements to a specific node and find the most important and relevant sections in order to justify and underpin his conclusions. Figure 21 shows such a summary:

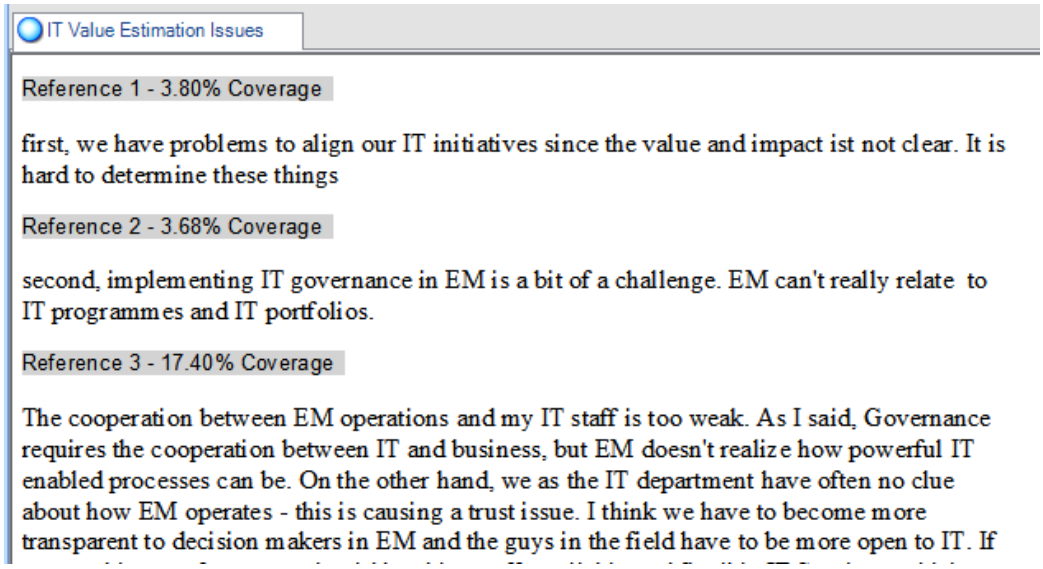


Figure 21: Reference summary per node

One of the major problems using NVIVO was its inability to rate the importance of a coded section. For instance, one section can be spot-on and gets straight to the point; a different section might be a bit fuzzy and describes the situation not very precisely. However, both sections will count as a full reference even though one section might be more valuable for the research's objective than the other might. To cope with this situation and stick to Mayring's Qualitative Content Analysis the researcher used the most important statements as "anchor examples" and attached them in the description of the specific node. This technique turned out to be very effective since these anchor examples were sufficient enough to design later models and methods without having to review the whole transcriptions.

6.1.3 Cluster Analysis

NVIVO's quantitative text analysis tools were used to identify clusters of interest for this research. The most useful tool was the tree-map. A tree map is a diagram, which illustrates the data as a hierarchical set of clusters that can vary in size and colour. One can use a tree map to compare the relative number of coding references to indicate the most frequently coded nodes, which are usually of major interest to the research's objective.

A larger rectangle indicates that the relative number of references in this node is rather high. The map is scaled to best fit the screen's resolution, so the

rectangles' sizes must be considered in relation to each other and not as absolute numbers. The colour of the rectangles indicates the number of resources used, whereas red indicates more resources than yellow and green (red- orange –yellow –green) (QSR International, 2010). Figure 22shows such an example:

Figure 22: Tree-Map / Node Cluster

6.1.4 Dependency Analysis in NVIVO

NVIVO's automated models allowed the researcher to identify dependencies between nodes and sources beyond the coding scheme. This was particularly useful to find patterns in the sources. However, in most cases the automated models had to be manually adjusted to be of use. Most automated models were too complex and relations and dependencies were hard to identify. Hence, the

initial models were stripped down to the main elements in order to reveal the most important relations and dependencies to draw conclusions.

The models are able to display:

- Children / Parent of selected nodes
- Relationships between nodes
- Sources coded of selected nodes
- Attribute values
- Node classifications
- Source classifications

Figure 23 shows an example of such a model. In this model the researcher wanted to find out which members of the “Focus Group” mentioned “IT Governance Issues”, including the child nodes. Therefore, this figure displays the parent and child nodes as well as the sources coded.

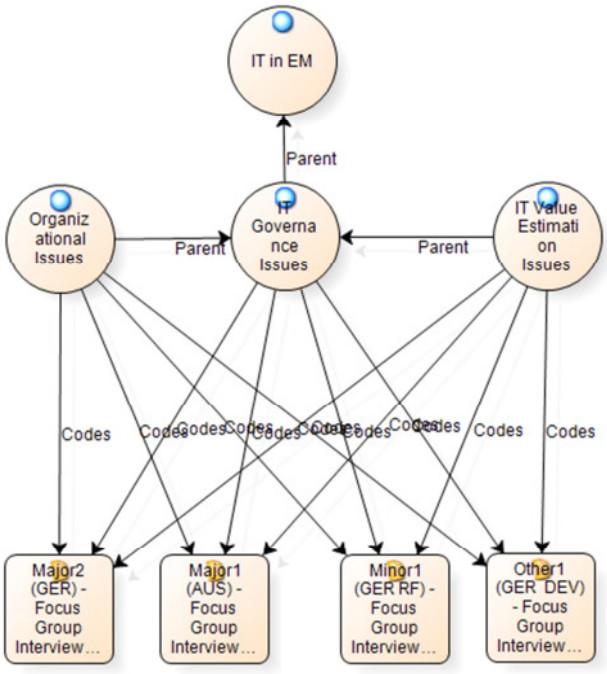


Figure 23: NVIVO model

6.2 Case Studies & Observation

Based on the findings from the previous research stages the researcher followed the hermeneutical research approach and drilled deeper into the

problem by the means of case studies. The selection of the case studies was made on size (> 50 employees) and complexity (stakeholder in multiple EM situations) of the organization. The reason for this selection was to ensure that all facets of EM/IT alignment processes can be studied. The decision fell on a large German municipality and an Australian state agency. Both organizations can be compared to a certain level since they fulfil similar tasks during a large-scale emergency or disaster. They are both embedded in federal structures and have to deal with multiple supporting agencies and organizations during a hazardous event. On the other hand, the two organizations differ in terms of possible EM situations they have to deal with and their associated impact on population and environment (e.g. Tsunami vs. nuclear plant incident, cyclone vs. effects of pandemic, city area vs. rural area, etc.), which enabled the researcher to compare the results from the two cases and draw more generic conclusions.

Primary concern of this phase was to get a thorough understanding of the processes in large EM organizations. Hence, the researcher started to analyse and model as-is processes on the basis of interviews, internal documentation, and observations. To visualize the organizational processes (before, during, and after a disaster) the researcher used ADONIS:CE, a software tool utilizing Business Process Modelling Notation (BPMN) and Universal Modelling Language (UML) (Karagiannis, 1995; Karagiannis & Kühn, 2002). The models were iteratively discussed with stakeholders of the organizations to identify inaccuracies, further issues, and possible solutions.

6.2.1 Major Case 1 (MAC1)

6.2.1.1 The Organization

Major Case 1 (MAC1) is an Australian EM organization acting on state level. They contribute to a safer, more resilient, and sustainable community by delivering services and assistance to approximately 5 Million residents. MAC1 leads and coordinates activities to minimize casualties and threats undertaken before, during, and after a disaster or emergency. It is also responsible for increasing disaster awareness within the community and actively engaging with

federal and local government to promote Emergency Management and volunteer management priorities. The department is not only responsible for EM procedures but also for ambulance services, fire and rescue services, and correctional services. The EM division consists of approximately 300 fulltime employees (FTE) and over 10,000 FTE including all other operational divisions. Additional information about MAC1 can be found in Appendix B (Major Case 1 - Documents).

6.2.1.2 IT Infrastructure

MAC1 has a very strong IT infrastructure. Their systems are linked and connected very well. One can see almost no IT islands, which is, according to their IT manager, one of the results of their IT Governance initiative. As an example, they integrated a capacity overview system for hospitals in all communication centres in order to achieve a better distribution of patients in case of a large-scale emergency by providing a real time operating picture of the status of emergency departments and available beds.

Moreover, they realized that they would need a centralized Emergency Operation Centre (EOC), which was opened in early 2011. It features state-of-the-art information and communication technology (ICT) to provide front-line staff with better information and coordination.

The EOC houses the State Disaster Coordination Centre, State Operations Coordination Centre, 24 hour Emergency Watch Desk, communication facilities for Ambulance Services and Fire Rescue Services, the Clinical Coordination Centre and the department's Geographic Information Services. With the integration of these services, they can coordinate and manage the situation with a pervasive disaster management system and, hence, increase the efficiency of staff and resources.

In general, the units of MAC1 utilize an extensive range of communications equipment (e.g. the dispatch service, radio, mobile data, paging, caller line Identification, station turnout and alarm telemetry). In addition to these primary systems, they utilize multiple secondary systems for internal financial and

business processes (e.g. budget management, asset management, and human resource management.

6.2.1.3 Organizational Structures

MAC1's structures can be describes as complex. Yet it is hierarchically organized and has clear responsibilities. Integration and coordination of and between other units and departments is not optimal but on an acceptable level. The following figure provides a rough overview of MAC1 organizational structure.

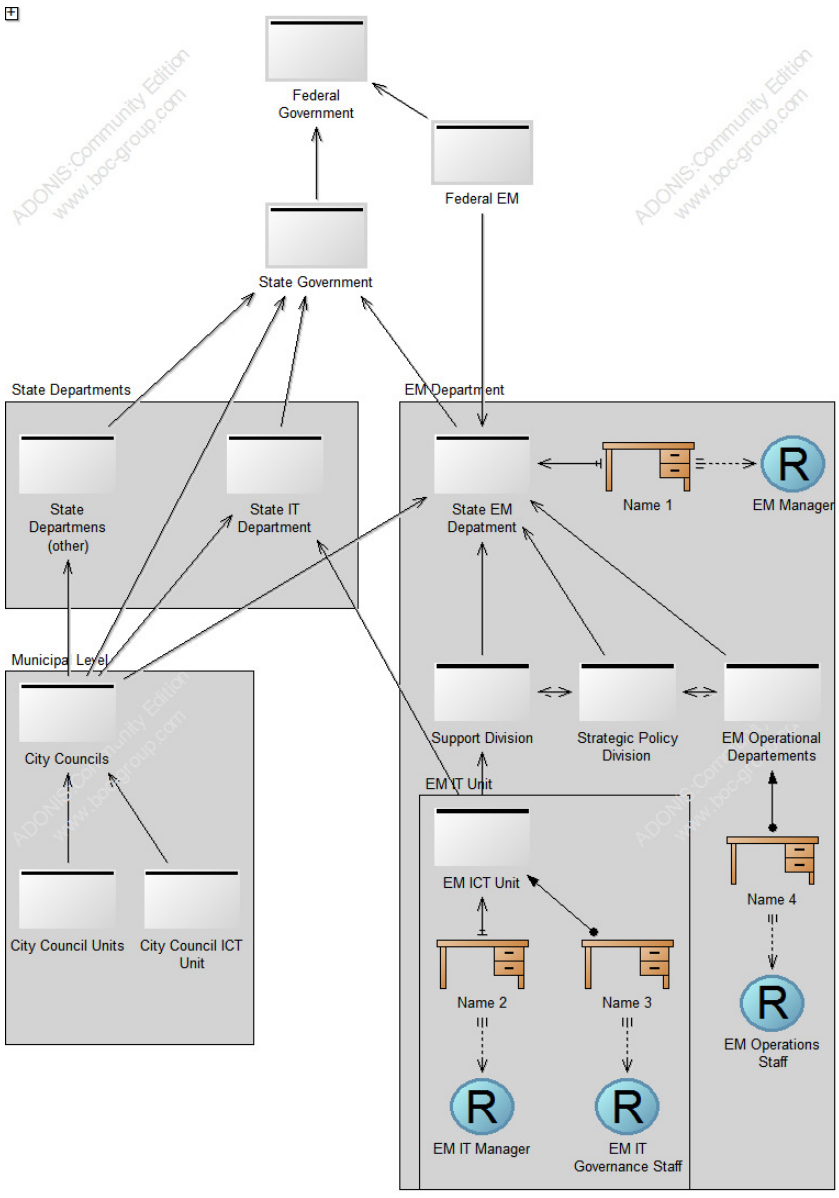


Figure 24: MAC1 - Organizational Structure

Due to new legislation in 2010, the organization is subject to revision of roles and functions within the Emergency Management division in order to improve their organizational structure and cooperation across departments and organizations. This is including changes to membership of units, modification of command and control roles, and strengthening of inter-organizational arrangements with federal, state, and local organizations. However, the general organogram as shown above will remain. One of these inter-organizational projects resulting from the cooperation and integration of systems across divisions was an “All Hazards Information Management (AHIM)” system. They had realized that it is important to provide up-to-data information to the right people, in the right place at the right time - not only within the organization but also to other divisions and organizations. Consequently, the AHIM programme has brought up sub-projects that streamline and synchronize inter-organizational IT initiatives to establish multi-channel information sharing capabilities, integrated command and control systems, and the synchronisation of the emergency services radio communication networks. Without a strong integration of other divisions and units in the IT related decision-making process, these projects would have never been as successful or even realizable.

The organization also realized that IT needs to be governed from different stakeholders within the division and, therefore, formed a “Communication and Information Committee”. The committee is responsible for the strategic governance of IT initiatives and has the responsibility to coordinate, monitor, and report to the executive level of the division about the performance of the IT programmes and portfolios. The committee’s focus lies on the delivery of “best value for money outcome” for these IT programmes.

6.2.1.4 IT Governance Maturity

The organization’s IT Governance maturity can be seen as advanced. However, it can also be said that the IT Governance approach was not driven by the EM division itself, but rather by the overarching governance body of the higher divisions. Nevertheless, MAC1 has realized the benefits of strategically aligned IT programmes and initiatives, and is fostering their “P3” approach

(Portfolio, Programme, and Projects). Therefore, the IT unit has implemented different roles, which support the communication between EM operations and the IT unit. This conjoint constellation allows them to identify promising IT initiatives and increases the trust of EM operations in IT enabled processes. Besides their “P3” approach, MAC1 uses ITIL and COBIT as IT-Governance guidelines. Their maturity levels vary from “Level 2” (partially defined) to “Level 4” (controlled) depending on the assessed processes.

With the Disaster Management Act from 2010 they agreed to integrate and enhance information and communication systems by an improved IT Governance body and continuous improvement processes for their Emergency Management systems. Moreover, to improve their IT service continuity they joined forces with other divisions and incorporated the government data centre as a member of its disaster management arrangement for critical ICT equipment.

MAC1 also agreed to implement essential planning activities with relation to IT in order to comply with financial and performance management standards. Annual IT planning activities are performed to update strategic plans and programmes. However, also quarterly and monthly reviews are undertaken in certain areas, which are seen as highly volatile and critical.

Since they had realized that EM operations are increasingly reliant on IT, they implemented a number of performance management systems including an audit issues tracking system, which helps them to improve systems and processes continuously.

The IT unit of MAC1 plans its IT activities based on the strategic direction of the EM operations and other corporate support divisions, which support the operational units. In addition, whole-of-government initiatives are also implemented and considered in this planning to ensure that all IT activities are aligned with and complement cross-agency objectives. The IT department also actively participates in the overarching Enterprise Architecture to ensure that the department’s strategic IT assets fit into this architecture.

All IT projects are governed by a project board, including major non-IT stakeholders and representatives of the IT department. The board’s purpose is

to manage the priority and scheduling of the IT portfolio against resource availability. It also ensures the value delivery of proposed investments and the portfolio alignment with strategic objectives of the department. For all new projects, the initiating unit has to ensure compliance with operational strategy and corporate requirements. Depending on size and impact of a project, it has to pass further gates controlled by the IT Committee and Finance Committee, which ensures that all projects are assessed for integrity of concept, funding, and capability to succeed. After initiation and approval, all projects go through a thorough project management lifecycle.

6.2.1.5 IT Governance / ITSM Issues

MAC1 has clearly the strongest IT Governance structure of all researched cases. Hence, their IT Governance / ITSM issues are limited and on a detailed level. Certainly, in every organization, space for improvement can be found, but since most of these minor issues are only on an organizational level, they are of no concern for this research project.

Nevertheless, MAC1 mentioned one major problem in their IT Governance and alignment processes. Even though they implemented steering committees and strengthened the cooperation between IT and EM operations, they still have problems aligning their IT initiatives since the added value of IT investment is hard to predict. Most prioritizations and value estimations are either based on financial indicators, which only cover the monetary perspective, or very subjective views. By using the steering committees, this subjectivity can be reduced. However, according to some of the employees, most IT initiatives are driven by the same people and a more objective approach would be desirable.

Another issue, of which actions are currently in progress, is the inter-organizational governance of IT initiatives. MAC1 and their close partners have realized that countermeasures and mitigation processes need the collaboration of multiple organizations. However, the cross-organizational alignment is still challenging and an ongoing task.

6.2.1.6 Conclusion

MAC1 has a strong IT infrastructure and strong IT Governance. During the case study and the comparison to other cases, it was realized that there is a progressive correlation between IT Governance methods applied in this organization and the strong and increasing utilization of IT enabled services and IT infrastructures. Key stakeholders of MAC1 confirmed that there was a reciprocal effect when they first utilized IT Governance methods in EM. As mentioned above, the initial IT Governance processes were more or less implemented under “force” of superordinate departments. IT Governance was seen as a necessity rather than an opportunity. In addition, IT was not very well implemented in EM operations. Unfortunately, no one of the interviewed staff at MAC1 had been working there long enough to describe the transition in detail, but the current staff assumed that older IT systems did not really fit into EM processes. Consequently, IT was not seen as an “enabler” for more efficient and effective EM operations. However, it was also said that today’s omnipresence of IT would not be manageable without a strong IT Governance in place. It was assumed that the involvement of EM staff into IT related decisions triggered an improvement process, which strengthened the utilization of IT. In turn, the higher IT utilization demanded a rigorous IT Governance and IT Service Management to maintain the quality of IT enabled EM processes. As a result, they realized value from their IT initiatives. Thus, it can be said that their structures and IT Governance processes have served as a role model for this research project.

6.2.2 Major Case 2 (MAC2)

6.2.2.1 The Organization

MAC2 is a municipality and one of the largest city-regions in Germany with approximately 3 Million citizens whereas 500.000 live in the inner city and 2.5 million in surrounding suburbs. The complete municipal administration is employing over 11,000 full time employees (FTE) whereas 500 – 600 FTEs work in the Fire and Rescue Department (FRD), which represents the major stakeholder in the “Virtual Emergency Management Team”. They are mainly

responsible for the planning before and the coordination during a large-scale emergency / disaster and take over the leading roles in strategic and tactical taskforces. They run a modern Emergency Operation Centre (EOC) and conduct emergency drills on a regularly basis. Since the city represents the state's capital city, they work closely with state level agencies and federal agencies. Moreover, MAC2 has realized that inter-organizational and cross-department cooperation become increasingly important in order to react to large-scale emergencies and disasters. Hence, they realized that conventional "emergency situation planning" is too inflexible to cope with different scenarios and changing conditions. Thus, they started to implement "Emergency Management Modules" (e.g. evacuation, supply shelter, etc.) on an operational level. These modules can be reused in different situations and define interfaces and responsibilities for the interactions within and across units. By combining these modules like 'LEGO' stones, they are able to react to very different situations by using standardized procedures. More details about MAC2 and their modules can be found in Appendix C (Major Case 2 - Documents).

6.2.2.2 ICT Infrastructure

MAC2 also has a relatively strong IT infrastructure. However, their EM related systems lack full integration, which is, according to interviewees, a result of three discrepancies: First, the separation of the day-to-day business (e.g. small fires, minor traffic accidents, and patient transport), EM procedures, and escalations levels. Second, the separation of the regular IT infrastructure from the city's administration and the technological islands of the FRD. Third, the legal separation between Police, FRD, and Ambulance Services (AS). However, the EOC makes first attempts to incorporate all these stakeholders. Even though their systems and are often not linked together the information can be at least forwarded "in-house" via conventional reports since all parties are represented in the EOC.

The EOC itself features a lot of technology, unfortunately Police representatives refused to disclose their IT infrastructures. During "normal" times, the EOC is mainly used as a dispatching centre for the Fire Department (FD), Ambulance Services (AS), and Traffic Control. The systems within the EOC are highly

redundant and secure. The EOC was known as the most modern facility of its kind in the beginning of the last decade and has proven its functionality during a large international sports event and an international political summit. The following picture shows the main room (left) of the EOC and the meeting room for the tactical/operational taskforce (right).

Figure 25: MAC2 - EOC Rooms

However, it must be said that particularly the large screen does look impressive in this picture, but during several visits of the researcher and during the observation of a pandemic drill the large screen was only used to monitor four traffic CTV cameras. During one of these visits, it was tried to show the researcher what this screen is capable of – unfortunately, this was not possible. It turned out that the system has not been used for a long time and that some of its functions were even offline. Additionally none of the attending operators felt confident with the system.

The Fire and Rescue Department runs most of the technologies, which are used in emergency situations. One of their core systems which is used is the electronic situation map (ESM). The ESM can provide user-specific views on tactical and operational levels. In addition, they have a communication module supporting their incident command system and a planning module, which provides predefined action plans for particular situations. The three systems are nicely integrated since they were developed and implemented by the same company. However, communications with other systems, particularly in an inter-organizational or cross-agency setting, are poor. As mentioned above most reports come from conventional channels (e.g. Phone, FAX, carbon paper reports, etc.). They have to be keyed in manually, which results in unnecessary delay and errors due to the media breach.

They also use an automatic alarm system for emergency situations. The system is used to contact stakeholders from all involved departments and CIPs. It is supposed to call these stakeholders automatically in order to alarm them, so they can initiate necessary countermeasures or preparations. However, this system is not well implemented. First, the database, which includes the contact details of these stakeholders, is not integrated into the city's LDAP directory. All details have to be maintained manually and are therefore often out-dated or full of errors. Second, the system itself is in development for over four years and is still full of bugs. Even though this system would provide major benefits and could reduce the responding time significantly, its development has been neglected or had at least not a very high priority. One of the interviewees said that this is probably the case since it was not seen as a "prestigious" project and other investments, which are "more seen" and "tangible", have been favoured.

6.2.2.3 Organizational Structures

MAC2's organizational structures can be seen as rather complex. For the day-to-day operations, the organizational structures are working quite fine. However, in the event of an emergency these structures are mixed up, which turned out to be a hindrance for good IT Governance practices. Figure 26 gives a high level overview of MAC2's organizational structure:

In case of and during an emergency, responsibilities shift from one department to another or escalate from local to state authorities (see Appendix C (Major Case 2 - Documents) for more detail on the escalation steps). This has two reasons: First, there is no designated EM department, which is clearly put into the hierarchical structure of MAC2. All EM plans and decisions are made by a "virtual" Emergency Management Team (EMT) consisting of the FRD, as the major stakeholder, and representatives of key departments within the city's administration, as well as representatives of CIPs, and in some cases advisors of the state government. Additionally, this team is only formed temporarily and has therefore only minor influence on the Information Systems and Information Technology architecture. The problem being is that they take over responsibility in case of a large-scale emergency or disaster but have to rely on IT decisions

from the day-to-day operations and permanent departments in MAC2's organizational structure.

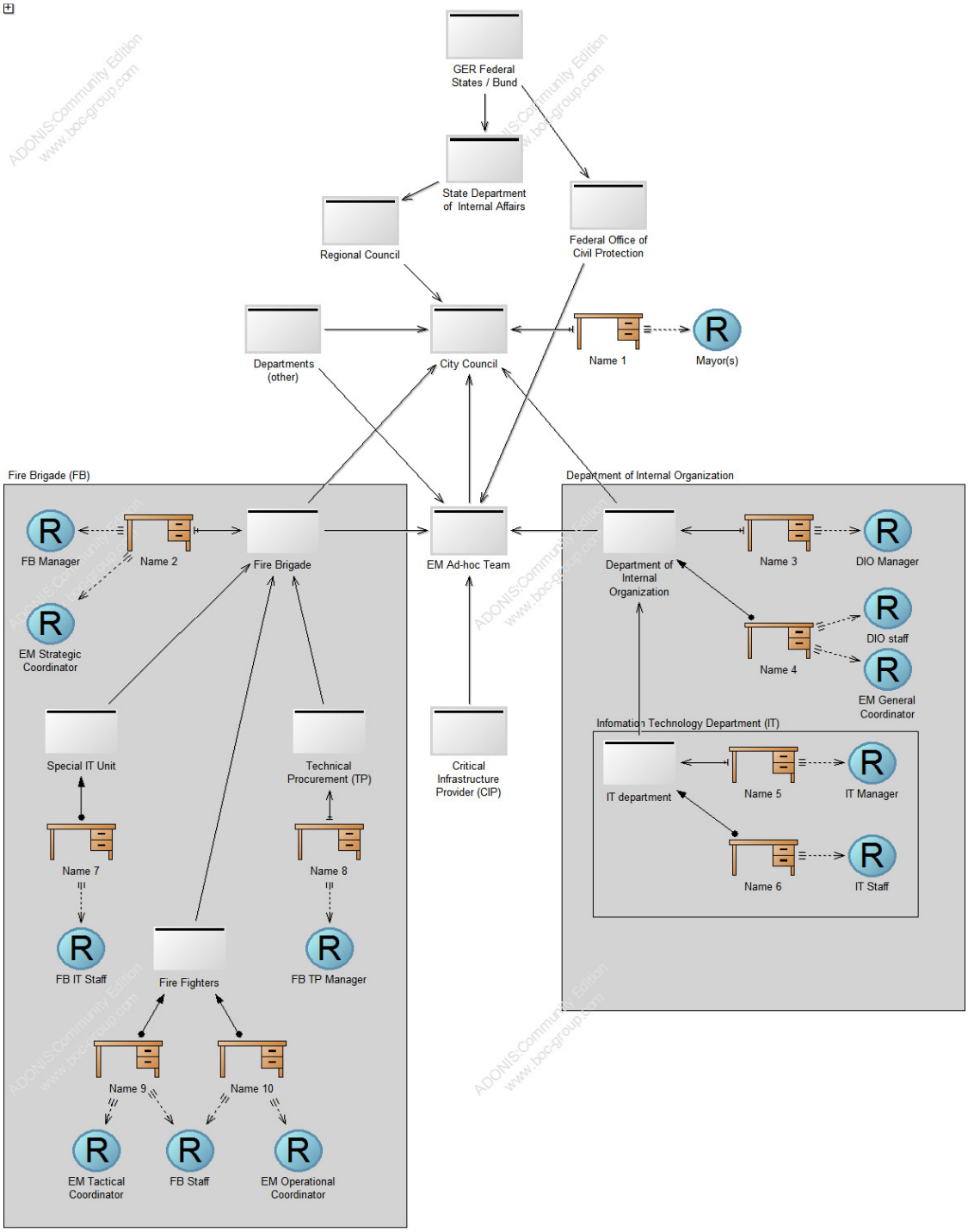


Figure 26: MAC2 - Organizational Structure

The second reason is the overlapping responsibility of the city's IT department and the FRD's own IT staff. The city provides basic IT infrastructures for the FRD, such as network and internet access, email services, LDAP directories, ERP, etc.). Even though the city's IT department runs most of the basic IT

functions and has rather mature IT Service Management processes in place the FRD has employed their own IT staff. The city's IT department sees itself as superordinate to the FRD IT staff. However, the FRD's IT staff argues that IT decisions of the city's IT department are often not suitable for the FRD's and EMT's requirements and that their procedures were too rigid. Consequently, there are tensions between the two units and the FRD's IT staff feel themselves forced to set-up their own IT infrastructures, which are decoupled of the city's IT infrastructure. Additionally, they argue that the city's IT staff would not be able to support their FRD and EM software and systems. On the other hand, they feel overburdened with the support of these systems since only 1.5 full time employees and some contractors are responsible for the FRD's and EMT's systems. As a result of this workload, they lack the time to manage their own IT proactively, which forces them to take a defensive position. Subsequently, systems such as the "alarm system" and "large screen" as described above are not well maintained and cannot be properly used. In turn, operational staff of the FRD and EMT do not trust most IT enabled processes and are reluctant to use new information systems.

Another issue, which was mentioned by some of the interviewees, was that a very strong character of FRD's operations owns the "Technical Procurement" function. Hence, the budget for IT initiatives is frequently cut and reused for technologies that are more "tangible" for FRD's operations since the value of information systems and underpinning technologies is not clear to the person in charge.

6.2.2.4 IT Governance Maturity

MAC2's IT Governance maturity cannot be generalized since the city's IT department and FRD's IT staff operate and plan differently. The city's IT is governed on a rather high maturity level (Level 2 – Level 4). The IT department and key-stakeholders of the city administration plan their IT initiatives together. They have a conjoint strategic vision about how IT initiatives should support the city's processes, good tactical plans to implement IT initiatives, and a strong performance measurement and IT Service Management procedures on their operational level. The city's IT department utilizes COBIT, ITIL, and BSI

standards to improve their IT value, IT service quality, and data security. However, FRD's and EMT's procedures are not considered in this IT Governance approach. Even though they are providing basic IT functions (network, internet, email, etc.) for the FRD, the most services are only designed and implemented for the day-to-day business. Moreover, most of the IT Governance and ITSM procedures are not applied in FRD since they are seen as "special". Hence, FRD's IT Governance maturity is on a much lower level (Level 0 – Level 1).

It seems as the FRD's IT staff is only seen as IT administrators not as process enablers. The value of IT is not clear to the decision-makers, moreover, their mistrust towards IT seems to be quite high. Therefore, IT initiatives and infrastructures are not very well integrated in their EM operations. The possible reasons and effects are explained the following paragraph.

6.2.2.5 IT Governance / ITSM Issues

The reason of FRD's low IT Governance maturity is most probably because their own IT unit is in a rather passive position. On the one hand, they complain about the rigid procedures of the city's IT department, and on the other hand, they "just fix things" and do not manage their IT proactively. The results are misaligned IT investments (e.g. large screen for the EOC, which seems not of much value to FRD's operations, VS. an alarm system, which could be of value but has not been implemented properly for more than four years). This poor value realization and IT service quality leads to a significant mistrust in IT enabled emergency processes. From interviews and documents of MAC2 the following major IT Governance issues emerged.

First, and probably most important, are the unclear responsibilities and poor cross-department / inter-organizational coordination of IT initiatives. IT related decision rights are not defined very well, which leads to the result that FRD's IT systems are not very well integrated and maintained even though the technical possibilities are provided by the modern EOC and the well maintained IT infrastructure of the city's IT unit. One of the reasons is that the city's IT department feels superordinate to the FDR's IT department, but when it comes to EM specific systems they refuse to take responsibility for these systems

since FRD has their own IT staff. The FDR feels that the city's IT does not support all their needs and that their procedures are too rigid and slow. As a result, they employ their own IT staff and pay the developer of the EOC system to maintain the software and infrastructure. However, this solution is obviously not optimal. Even though they do not need to rely on rigid and slow procedures of city's IT department, they are not able to realize the full value of their systems or maintain their functionality on a satisfactory level. It is therefore necessary that IT units, city administration, and FDR/EM operation discuss future IT directions and initiatives together (whereas all stakeholders enjoy equal rights) in order to find conjoint solutions and create a symbiosis between IT, EM, and the day-to-day business. FDR's IT specialists seem to have a good understanding of EM processes but would need the support of the city's IT department to cope with the systems complexity. Consequently, they could be used as a catalyst to align the city's IT with FDR's requirements.

The second issue, which was mainly mentioned by the FDR's operations, were the non-transparency of the current IT systems and procedures. The alien terminology of IT experts and the complexity of the city's IT regulations is a barrier for EM operations involvement in IT related decisions. It is therefore important to use simple, flexible, and understandable best practices and procedures to implement IT Service Management and ensure the quality of IT enabled EM processes.

The last major issue is the value estimation of IT initiatives. Besides the organizational issues of MAC2, they also lack a balanced IT portfolio, which is supporting their strategic goals. IT investments are based on "gut feeling" of only a few individuals, which results in very subjective views. Moreover, in some cases it was reported that the very same company who is maintaining the systems at the EOC is also consulted to write the functional specifications for future IT investments. Therefore, it is questionable if the requirements are defined by the FDR's operations or rather by the interests of the company. A more transparent and objective IT value estimation method would help the organizations to come to more replicable and reasonable findings, which could be used to prioritize their IT initiatives an build an balanced IT portfolio.

6.2.2.6 Conclusion

MAC2 has a modern IT infrastructure but a rather weak IT Governance, at least in the FDR's and EM's area of responsibility. Hence, their systems are not well integrated, which leads to a low value realization and adoption of IT initiatives. Consequently, their operational process are sub-optimal and trust in IT enabled processes is rather low. Compared with MAC1's strong IT Governance and high utilization and integration of their IT they clearly underperform in this area. Nevertheless, this confirms the correlation between IT Governance and IT utilization, which was presumed in MAC1.

However, it must be said that MAC2 is using novel approaches, which make their EM operations quite flexible. Their "modular approach" instead of a rigid "emergency situation plan" is particularly useful to identify recurring procedures, which can be automated or at least supported by IT services. In order to unfold the maximum value of IT initiatives, processes have to be repeatable. Even without a sound IT Governance in place, they realized that universally applicable IT systems are often of more value than IT systems, which are tailored for only one particular situation. Moreover, the complexity of such modules and processes is much lower compared to a full emergency situation, which, in turn, should make it easier for IT and EM personnel to evaluate the impact and risk of IT services for their operations.

6.2.3 Minor Cases (MiC 1 – 4) – Summary

Since the four minor cases have not been researched in the same detail as the two major cases, their presentation and the conclusions drawn are summarized in this chapter.

6.2.3.1 The Organizations

MiC1

The first case study was chosen to see how larger non-for-profit EM organizations utilize and manage IT. MiC1 is a flight rescue service in Germany. They operate 31 helicopter / airplane bases in Germany, Austria and Denmark, with approximately 60 air vehicles. They support emergency

missions and take care of the transport of intensive care patients. MiC1 works hand in hand with ground-based emergency services and hospitals and is committed to high quality standards in flying, technical equipment, and medical care. In order to maintain and provide such high standards and improve their services continually they implemented an internal quality management system, which defines how employees of the different departments can organise all their workflows and optimise them. In addition to their internal endeavours to improve their operations, they frequently work with universities and research facilities in projects to improve their technologies. The combination of the technological pioneering role and their quality management system caused a rethinking of their IT operations and management.

MiC2

MiC2 is a local Red Cross chapter and located in the suburbs of a major city in Germany. It was chosen to investigate how small EM related organization work and cope with IT issues. As second aspect was to see how its internationally acting federation of Red Cross and Red Crescent societies supports such a small chapter. Approximately forty volunteers, who spend around 6500 hours on duty per year, run the local chapter. Even though their main tasks are paramedic services for smaller incidents they are also playing an important role as first responders in emergency situations. They do not spend much money on IT services, hence, IT systems are not really managed. The few technologies they use are maintained by a volunteer who is privately interested in IT.

MiC3

The third minor case is about a critical infrastructure provider (CIP) working closely with municipalities, state agencies, and federal agencies. MiC1 is an energy company running nuclear power plants, fossil-fired power stations, and hydroelectric power stations across Europe. Following their code of conduct, they have implemented a sound IT, compliance, risk, and crisis management. Their crisis management gave input on several federal crisis and civil protection guidelines. MiC3 was chosen to see how CIPs are integrated in EM procedures and how they communicate with municipalities and first-responders prior and during an emergency. It was also interesting to see how such organizations

perceive the IT capability of EM organizations and related administrations from an external point of view.

MiC4

MiC4 is the last case study, which was conducted in a chemical plant in Germany. The case was chosen to see how “possible points of peril” are integrated in EM procedures and how they communicate with authorities and first-responders before and during an emergency situation. MiC4 runs a chemical plant producing solar cells. They have an extensive use of chemicals in their production facilities. Since they are located in a large industrial park amongst other chemical plants and industrial manufactories, they have to fulfil a set of security precautions and have to implement early warning systems and procedures in cooperation with the operator of the industrial park and local fire and rescue services.

6.2.3.2 ICT Infrastructure

The IT infrastructures of the minor cases vary largely. Therefore, it would not make sense to go into detail. However, identical issues can be found particularly in the inter-organizational communication.

MiC1’s IT infrastructure can be seen as sophisticated. Flight rescue and the coordination of patient transports demand integrated logistics systems with participating hospitals. However, this high utilization of IT infrastructure was not always the case. According to interviewed staff members, IT systems were not as efficient and reliable before the new IT Management was in charge. They fostered the utilization and integration of IT systems within and outside the organization. Now they have seamless and paperless documentation of their patient records and can even send vital functions of patients in real-time to most hospitals from their airplanes and helicopters. However, it must be said that these IT initiatives were not driven because administrations or other EM organizations saw this as a necessity. It is rather because MiC1 is financing their endeavours by regular patient transport (e.g. a patients needs to be transferred to different hospital in order to receive the right treatment or

surgery). Moreover, it has to be mentioned that MiC1 is communicating mostly via radio with other EM organizations, which is causing problems in EM situations since they do not have all necessary information readily available. One example, given by an interviewee, which was causing enormous trouble was that a first responder had given the duty officer of MiC1 coordinates via radio, but accidentally inter-changed the numbers. Consequently, the helicopter went to the wrong destination and precious time was lost. An integration of GPS devices in one of the first-responders cars with MiC1 GPS service used in the helicopters might have been able to prevent this confusion.

MiC2, the local Red Cross chapter, is barely using IT for their missions. The most used information sources are their radio and alarm devices. Occasionally they use simple personal computers and a self-maintained website to track and document their operations. This basic IT infrastructure is mainly the result of the voluntary commitment of MiC2's staff. However, they also indicate that there is not much support from the higher or regional chapters within the Red Cross organization regarding IT initiatives and support. In their view, the upper hierarchies should give more IT support and infrastructure to local chapters since they have not the resources and knowledge to do it themselves. The volunteers of MiC2 have generally a good understanding of the capabilities of IT services. They particularly miss the ability to communicate with other first-responders in large-scale situations. One interviewee mentioned that the use of mobile devices with a link to a general situation map would be most helpful. This would enable them to see were roads are blocked or bridges collapsed and even update such information to support other fist-responders.

The CIP (MiC3) has the largest IT infrastructure but almost no IT interfaces to EM organizations and authorities. Communication is done mainly via conventional channels. According to MiC3's crisis manager, there are two major reasons. First, the IT infrastructures of first responders and authorities are too heterogeneous. MiC3 is primarily a for-profit organization and the integration and maintenance of such systems would simply reduce their profit. Consequently, if such IT initiatives are not driven by the authorities or leading EM organizations there is no point for the CIP to invest in such systems, particularly if they are not unified. Second, the CIP does not trust external IT

systems since most of them are not run at a professional level and lack accepted certification. Security protocols and procedures have to be compliant with the CIPs regulations, however, no efforts have been made by the authorities or EM organizations to find conjoint solutions. During a nuclear incident drill the lagging communication, which was caused by the lack of integrated systems, was one of the major problems since authorities made decisions on out-dated information provided by conventional communication channels.

MiC4's internal IT infrastructure is not very large but based on cutting-edge technology. They were also forced to integrate internal early warning systems (sensors that measure particular chemical emissions) into the industrial parks infrastructure in order to enable them to take preventive actions or counter measures. The integration was not done on a voluntary basis, it was obligatory for them in order to comply with the industrial parks legislations. However, this integration enables the first-responders in the area to react much faster and more precisely, but it also demands conjoint decisions about the underlying IT infrastructure and maintenance procedures.

6.2.3.3 Organizational Structures

As with the IT infrastructure, the organizational structures are quite diverse in the four minor cases. However, what was learned in all of these organizations was that the best IT decisions were made conjointly, either between IT and EM operations to increase the reliability and utilization of IT (MiC1), or between organizations to increase information richness and reach (MiC1 and MiC4). MiC1 has in contrast to MiC2 an IT infrastructure, which is supporting their operations quite well. However, this was only the case because the new IT Management had started to "ask operations" what they need and integrated them in crucial IT decisions. Moreover, MiC1 and MiC4 were forced to integrate their IT systems in order to react faster; this was only possible because they started to discuss possible IT solutions and future IT directions together. In contrast to these positive examples, MiC3 depicted a negative example where the non-integration of systems, caused by the unwillingness of first responders

and administrations to find mutual IT directions with the CIP, lead to wrong decisions.

With regard to internal IT Governance structures and decision rights, three of the four cases are either using IT steering committees or have at least a strong partnership between the business and IT in order to align their IT systems with their strategic goals. However, their IT Governance structures were not implemented to support their EM processes but rather their business goals since all three cases (MiC1, MiC3, MiC4) are also financially driven. Their strong internal IT infrastructures and integrated systems are a result of their "core business" (commercial patient transport, energy production and trade, and production of solar cells). EM procedures and associated IT initiatives are mostly of no concern to their decision makers unless they are driven by the authorities or primary EM organizations. Consequently, the integration of systems and the inter-organizational information exchange between participating organizations is often sub-optimal. The researched companies and organizations are not generally against a better integration but they expect authorities and other EM organizations to follow IT standards and provide competent contact persons in order to come to conjoint and safe agreements about future IT directions and initiatives.

6.2.3.4 IT Governance Maturity

With regard to the IT Governance maturity levels of the researched minor cases, two of the four cases (MiC1 and MiC4) have a medium maturity (Level 2 – Level 3), the CIP (MiC3) has a very high maturity (Level 2 – Level 5), and MiC2 – the local Red Cross chapter – is not even aware of IT Governance or IT Service Management method. Hence it uses no framework at all (Level 0). Most of the other researched minor cases use ITIL as a guideline, only MiC3 uses COBIT, SixSigma and CMMI as additional frameworks.

The CIP, as a stock exchange registered company, with a holding structure and several affiliated companies has certainly the highest standard. They are aware that aligned IT systems can add value to their processes. Hence, they use steering committees, strategic plans, business cases, IT portfolios, and project stages to govern and manage their IT initiatives. However, EM processes are

seen as unimportant since they are not adding value to their core business. Their involvement in EM processes are is only a legal obligation and integration of information systems with administrations an EM organizations is not wanted unless they benefit from it. Moreover, in their perspective the integration of information systems bears a huge risk for their operations since they question the ability of administrations and EM organizations to manage their IT systems properly. They would only accept an integration if these organizations and authorities would apply the same IT Management and security standards. It could therefore be said that they internally value IT Governance methods and continuously try to improve their processes but regarding EM processes they only see value if the maturity level is equal across participating organizations and if the benefit from an integration.

MiC1 and MiC4 have started to realize that IT Governance and IT Service Management methods can help them to choose the right IT initiatives and preserve the value of their IT investments by delivering effective and efficient IT services to their operations. Both have inter-organizational arrangements to integrate their IT systems to become more effective.

MiC2 has the lowest IT Governance level of the researched cases. However, the voluntary staff is complaining about the low IT integration and would wish that the upper hierarchies would put more effort in applying and supporting IT services and infrastructures. It is obvious that they cannot implement technologies and management structures themselves due to their size, but since they are technology savvy, they would be able to utilize IT with the help of the whole-organization and consequently improve their processes.

6.2.3.5 IT Governance / ITSM Issues

In contrast to the major cases the IT Governance and ITSM issues of the minor cases are different since they have less planning activities and are more focused on supportive tasks in case of an emergency. Two of them are private organizations and do not participate actively in rescue missions, the other two organization are involved as first-responders but largely rely on the decisions of administrations and superordinate EM organizations, which are involved in

strategic and tactical planning to avoid, prepare for and respond to emergencies.

Even though very diverse, all minor-cases share one major issue: The lack of inter-organizational IT co-ordination for EM processes. Some of them have a strong IT Governance for their core business, which allows them to align and maintain their IT initiatives quite well. However, all of them complain that they are missing a shared IT vision and governance across the participating organizations. Infrastructures and processes are too heterogeneous to integrate IT services and technologies. Consequently, information richness and reach are sub-optimal. Moreover, they criticize that key administrations and EM organizations do not comply with accepted standards and best practices, and do not provide competent contact persons or committees in order to streamline and coordinate the IT infrastructure and information management. Hence, some of them would propose, or at least support, an inter-organizational committee to steer IT initiatives across EM organizations involved.

An additional problem, which emerged from MiC1 and MiC2, was that they feel overwhelmed by existing IT Governance and ITSM practises. Even though, MiC1 has implemented basic functions, roles, and processes of ITILv2, they complain that they had a hard time to adapt these best practices into their IT Management. After showing MiC2 examples of the ITIL books, they just said that this would be too much for them to read, but they are not refusing to use such “best-practices” per se. However, such practices have to be simple and supported by the upper hierarchies.

6.2.3.6 Conclusion

The minor cases differ largely from the two major cases because of their different focus. Nevertheless, it was important to research them and get whole view on how the different organization types are involved in EM processes and where they have issues regarding the utilization and governance of IT. The two major cases are involved much deeper in the planning and coordination before, during, and after a disaster struck. Hence, the strategic planning of IT and the associated organizational and methodological issues are more complex. However, as MC1 and MC2 have confirmed, the inter-organizational integration

of “supportive” organizations, such as CIPs, volunteers, and privately run companies is increasingly important to improve EM processes. A key factor is the integration of IT systems to increase information richness and reach in order to address the right people, with the right information, at the right time. However, the minor case studies have shown that such an inter-organizational IT Governance approach is missing. Consequently, there is no shared vision of IT services, IT infrastructures, IT standards, and procedures. Moreover, due to these missing links privately run companies and volunteers question the IT Management capabilities of authorities and primary EM organizations since they often do not provide competent contact persons for IT related questions. However, it must be said that three of four minor cases have either a medium or high IT Governance maturity level, which indicates that they are realizing value of IT Governance and ITSM methods for their daily business. However, this governance is missing on an inter-organizational level. Therefore, it can be assumed that these issues have to be resolved by external and superordinate administration and organizations such as major case 1 (MC1) and major case 2 (MC2).

6.2.4 Drill Observation

6.2.4.1 The Situation

The researcher observed a pandemic drill in Germany, which was conducted over several months and had its peak in a two-day full exercise in 2009. The drill was based on the experience collected during the previous bird flu and swine flu infections.

Different EM related organizations and authorities took part: Police departments, fire departments, ambulance services, local government agencies, regional government representatives, state government agents, the public health department, hospitals, volunteer first responders, banks, critical infrastructure providers (CIP), and even private companies.

In the early stages of the drill, only reports about casualties and possible preparations were sent out. A “Drill Committee” decided about the progress and direction of the drill. Hence, they staged the general setting of the drill and sent

out additional reports containing “side quests” for the participating organizations (e.g. contaminated water, riots, road blocks, lootings, etc.) towards the end of the drill and particularly in the final two days of the exercise.

Main venue, where most strategic and tactical countermeasures and preparations were decided and planned in the final two days, was a large and modern Emergency Operation Centre (EOC). The researcher observed the drill only on the last two days of the exercise but had the opportunity to screen all the reports from the previous months in order to get the whole picture and understand the situation and reactions of the participating organizations.

6.2.4.2 ICT Infrastructure

As already mentioned, the final two days of the drill were mostly located in a relatively modern EOC. Hence, all basic IT functions (e.g. networks, internet, printer, etc.) were provided. Additionally, the strategic and tactical taskforces were able to use the Fire and Rescue Department’s (FRD) infrastructure including their special systems (e.g. electronic situation map, electronic report documentation, large screens, projectors, etc.). The operational parts of the EOC (e.g. the emergency hotline) were not fully affected since they had to provide the regular functions of the EOC to the public.

However, the most interesting observation during this drill was not “which IT services were there” but rather “which IT services were NOT used” or “which IT services did NOT work”. During the exercise a couple of IT related problems emerged. The following list will give a short overview to explain the situation:

- Reports came in on carbon paper and had to be keyed into the electronic report documentation system. This resulted in errors and lag. Moreover, some of the carbon paper reports were not legible. Hence, reports could not be used for the decision-making process on tactical and strategic level. Consequently, decisions were based on incomplete or out-dated information, which led to wrong decisions. Furthermore, since the carbon paper based process did not give feedback to the reporter, he/she considered their report as processed and went on with their operational activities.

- The same happened with reports coming in via FAX, some of these reports were put into the FAX-machine upside-down, which resulted in an empty report. In the best case, somebody had to follow up the source and ask to resend the report; in the worst case, they were laid aside for later revision and forgotten.
- Even though the EOC was able to provide the resident organizations internet access, they were not able to set up a de-militarized zone (DMZ) for participating CIPs and other organizations, who were working in the strategic and tactical taskforces. They had to use 3G mobile devices in order to get access to the internet. In some cases Virtual Private Networks (VPN), had to be used in order to access data from their own organization or company. This turned out to be a major problem since the “Drill Committee” decided to send out one of their “side quests” in which the 3G networks broke down due to a network overload (e.g. this can occasionally happen on New Year’s Eve due to an increased usage of SMS, tweets, calls, etc.). Consequently, representatives of CIPs and other organizations had to leave the taskforce in order to proceed with their duties.
- Instead of using the large screen of the EOC to display the general situation, up to eight people were sitting around a monitor to check the electronic situation map, which was not very effective.
- Taskforce members, who did not permanently work at the EOC were not able to print.
- IT staff was not on-site to fix systems.
- As mentioned in MAC2, the alarm system did still not function.
- Generally, the whole communication between organizations did not function properly.

6.2.4.3 Organizational Structures

Since multiple organizations took part in the drill, there was no permanent organisational structure. However, it became clear that particularly other organizations outside of the EOC are not well integrated. The organogram shows that mainly administrational departments and FRD units are present in

the taskforce and communication with other organizations is done via the EOC and official reports. Unfortunately, the police of the EOC refused to work with the researcher, but from statements of other EOC personnel, it became evident that they are running a similar taskforce structure in parallel.

The following figure will illustrate how strategic taskforces, tactical taskforces, on-scene operations, governmental departments, and external organizations worked together.

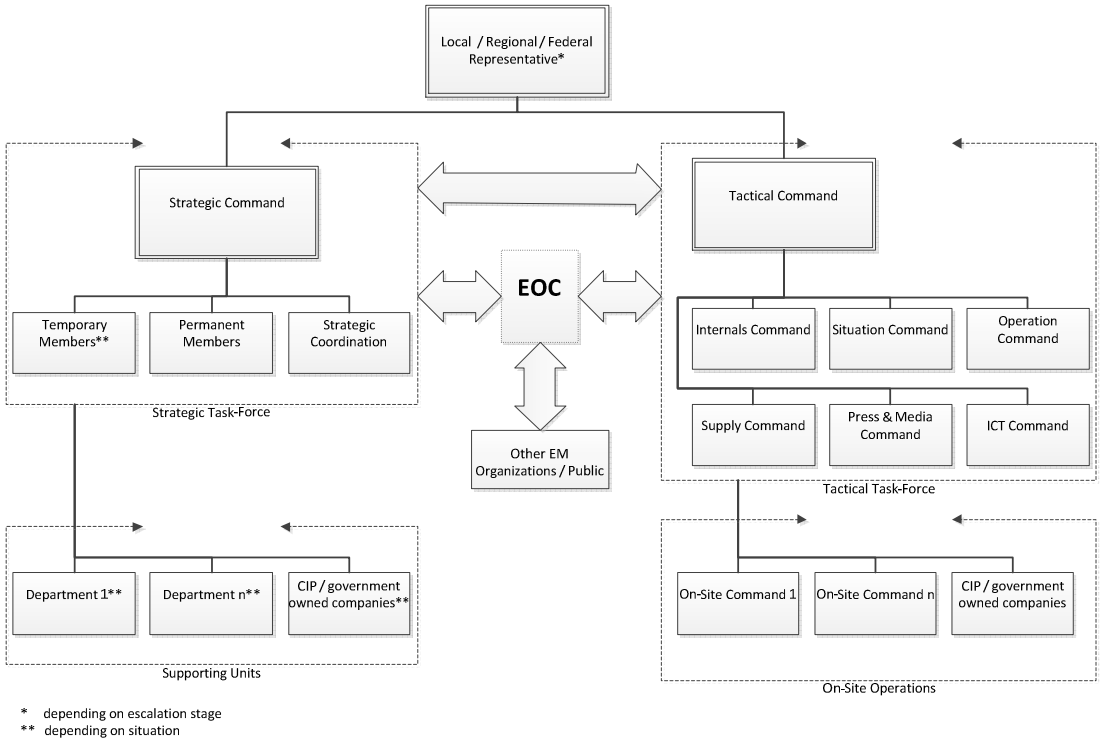


Figure 27: Drill Organization - Strategic, Tactical, Operations, Support

6.2.4.4 Conclusion

During the drill observation, some of the assumptions of the case studies and interviews have been confirmed. Moreover, the researcher's perception of the generally weak information processes, systems integration, and inefficient organizational structures were confirmed by representatives from the participating authorities in their final report. The taskforces were unable to predict trends and to make forward-looking strategic decisions. Threatening situations were underestimated to some extent and EM operations did respond too slowly or not at all. Even more interesting was the finding that some authorities made contradictory decisions based on different information, which

in turn led to even more confusion amongst the participating organizations and taskforces. The researcher's conclusion that some of these issues could have been remedied or at least mitigated by a proper information management supported by the right technologies and organizational structures was also confirmed in the "Drill Committee" final report.

Besides these inter-organizational issues, the low quality of IT Services also became evident during this drill observation. Several, IT issues occurred during these two days, which could have been prevented or at least been solved much faster, if the responsible EM organization would have had stronger ITSM procedures.

Moreover, it became clear that some of the IT investments made add almost no value to EM operations since they are not utilized in their procedures. It was the researcher's impression that EM personnel deliberately avoided the utilization of IT in their processes and tasks. Thus, it can be said that there was a gap between which IT services would have been need by EM operations, and which IT services were delivered. It can therefore be concluded that these IT initiatives are misaligned with EM operation's requirements because of weak IT Governance processes within and across EM organizations.

7 General Findings from the Qualitative Data

The analysis of the interviews, cases studies, and observation was done in isolation in the first place. However, to develop conceptual IT Governance models and methods for the EM domain, these findings had to be combined and generalized. The following chapter will describe this generalization process and the findings.

7.1 Identified IT Issues in EM Organizations

As stated in the introductory chapters, the domain of Emergency Management (EM) is not comprehensively researched yet. In particular, the domain's issues regarding the alignment of IT initiatives with EM's strategic goals as well as the utilization of IT Governance and IT Service Management methods have not been analysed thoroughly until now. Hence, it was one of the research objectives to identify the importance of IT Governance related issues for this domain. Consequently, the first stage was to find out if the research objectives are valid and important for this domain.

From the first interviews with EM experts, the researcher has identified their Top10 IT Management issues shown in Table 4(Vogt, Hales, Hertweck, & Finnie, 2010; Vogt, Hertweck, & Hales, 2011).

Rank	Node	Sources	References
1	Lack of interoperability of systems	6	52
2	Lack of responsibility for IT	6	48
3	Lack of IT alignment & IT value methods	6	42
4	Lack of appropriate IT service management	6	41
5	Un-improved processes	5	39
6	Fuzzy (or non) service levels	6	38
7	Lack of importance of IT to EMs	5	32
8	Lack of transparency of IT to EMs	4	30
9	Lack of flexibility of systems	5	28
10	Lack of reliability of systems	6	27

Table 4: Primary IT Issues in EM

The table shows the results of the first NVIVO coding scheme. It reveals very interesting findings from the early stage of this research, which are still valid. Excluding technical issues such as interoperability (1), unimproved processes (5), inflexible (9), and unreliable systems (10), all remaining issues can be related to IT Governance.

One remarkable finding was that all participants gave examples of “Lack of IT alignment & IT value methods”, “Lack of responsibility for IT”, and “Lack of appropriate IT Service Management”. All three categories play a major role in IT Governance (Brenner, Garschhammer, & Hegering, 2006; Y. E. Chan, 2000, 2002; Guldentops, 2003; IT Governance Institute, 2008c; Jacoby, 2009; Marrone & Kolbe, 2010, 2011; Symons, et al., 2006; Van Grembergen & De Haes, 2009; Venkatraman, Henderson, & Oldach, 1993; Weill & Broadbent, 1998; Weill & Ross, 2004).

It is also interesting to note that these issues are recognized as priorities in both German and Australian organizations, which indicates that this is possibly a universal issue and not only the problem of a particular governance system or organizational environment.

Considering these results, it can be said that IT Governance related issues are relatively important to EM organizations. Therefore, it was assumed that improving IT Governance methods could have a positive impact on the performance of Emergency Management processes. This assumption was confirmed during the case studies and follow-up interviews, where the researcher found indicators for a connection between the IT Governance maturity, the utilization of IT in EM processes, and the information quality and speed (see Figure 28).

Certainly, the sample of only six EM related organizations is not necessarily representative for the whole domain. However, since such relations can also be found in companies in the private sector, public administrations, and non-for-profits, the relation between these components in EM related organizations can be seen as valid even though they have a slightly different angle (Bhattacharjya & Chang, 2007; Luftman, 2004; Schwabe, 2009; Sethibe, et al., 2007; Simonsson & Johnson, 2008; Weill & Ross, 2004).

The following chart shows the relationship of the three dimensions in the researched cases.

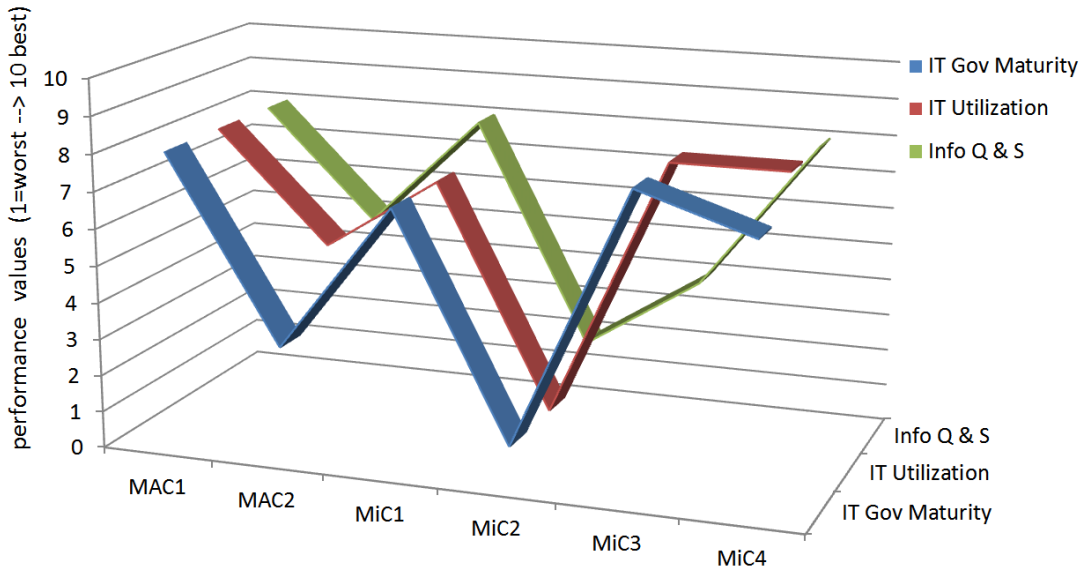


Figure 28: Relationship of IT-Gov Maturity, IT Utilization, Information Quality & Speed

The graph reveals that in all cases a low IT Governance maturity causes a low IT utilization, whereas a high maturity level is associated with a higher IT utilization. The same is true for information quality and speed (Info Q & S), even though in one case (MiC3) the “Info Q & S” value is much lower than the IT Governance maturity and the IT utilization. However, it must be said that the internal non-EM related “Info Q & S” value is very high, only the EM related information flow to external authorities is rather bad since the they were not able to provide appropriate interfaces for MiC3.

Moreover, because of the tight relation of IT Governance and IT Service Management, as explained in Chapter 2.2 (Figure 3, p.35), it was concluded that tackling IT Governance issues in EM organizations will also have a positive influence on technical issues (cp. Salle, 2004; Simonsson & Hultgren, 2005). This assumption was also confirmed by some of the interviewees and secondary data, who reported about how the reliability of the systems increased after the IT Management implemented IT Governance and ITSM methods, and how unreliable systems affect the utilization of IT in EM operations. Example statements were:

- “I’m not an IT expert, but the exchange of your IT Management caused that now things are handled differently. What they do is more structured and focused; this certainly helped us to improve our own services”.
- “Some people just don’t trust IT because they fear it is unreliable, others won't use IT because they don't understand it…. I understand their position to some degree and I think they are trapped in a circle. Since IT hasn’t much relative importance in most EM organizations, it isn’t managed very well. Consequently, those IT systems are not very reliable. If a system is not reliable it has no or lesser value for EM operations”.
- “Also, EP&R has not fully updated its enterprise architecture to govern the IT environment. As a result, during significant disaster response and recovery operations, such as the 2004 hurricanes, IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities. Such problems usually are due to FEMA’s focus on short-term IT fixes rather than long-term solutions. Inadequate requirements definition, alternatives analysis, and testing prior to systems deployment are characteristics of this reactive IT Management approach.”(Department of Homeland Security (DHS), 2005, p. 8)

7.2 Identified IT Governance Issues in EM Organizations

IT Governance issues (alignment, responsibility, and service management) were identified as a primary issues in EM organizations (cp. Table 4, p.147)), but are also known as factors for organizational success (Marrone & Kolbe, 2011; Venkatraman, et al., 1993; Weill & Ross, 2004). Therefore, the researcher examined these issues in more detail in the second set of interviews. The questions focused primarily on how IT decisions are made, what factors are used to prioritize IT initiatives, and how IT enabled processes perform in the view of the interviewees, and what has been done to manage such IT services.

A typical question for this set of interviews was for example:

- Do you have an ICT Governance body? If “Yes” what ICT governance Frameworks are you using and how is your process maturity? Did you make adaptations to those frameworks? If “yes”, explain them and give reasons.
- Briefly explain your organizational diagram and describe the major tasks of the important units for EM processes. How does your ICT unit fit in?
- Do you have an IT investment / project portfolio? If “yes” what does it look like? What are the factors for prioritization? If “no” why don’t you make use of a portfolio?

Characteristic answers to this set of interviews were:

- “Look at the size of these publications. They are just too complex; I don’t have the time to read thousands of pages”. “EM is different from industry, these frameworks focus too much on monetary goals”. “I’m a Fire-fighter not a Hacker, the terminology used doesn’t relate to my daily work”.
- “I think one of our biggest problems is that nobody feels responsible for IT decisions in emergency processes. IT says it’s our baby since they think we have totally different processes compared to the day-to-day business. We know our structures, but we don’t have a clue about IT. That’s an issue if it comes to planning”
- “The EM unit is buying things that do not fit into our infrastructure. E.g. they have spent thousands on a high availability system without considering the capabilities of the network and the server room”. ”I wish I could estimate the impact of an investment more rigorously. We’ve spent a lot of money on things that turned out to be less useful”

Figure 29 summarizes the findings of this research stage and identified the main IT alignment issues in EM organizations and their difficulties with existing IT Governance methods.

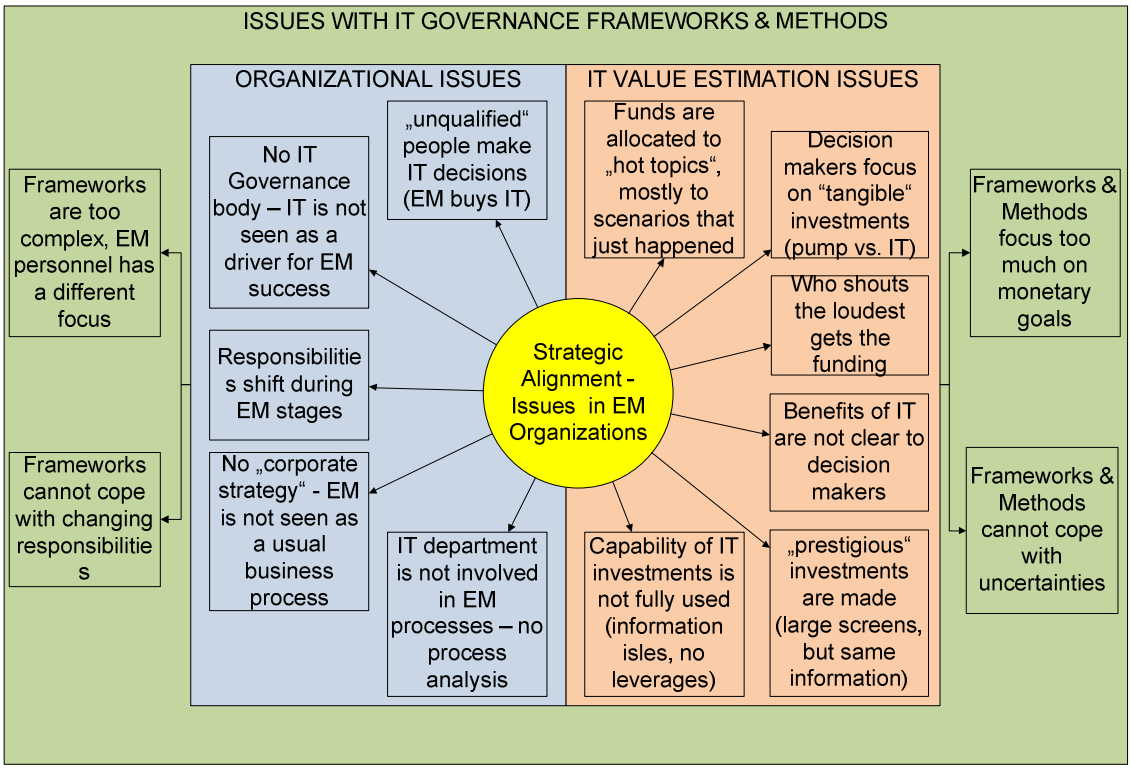


Figure 29: Strategic alignment issues in EM

As one can see, the issues could be separated into three main sections:

1. Issues with existing IT Governance Frameworks & Methods (green)
2. Organizational Issues (blue)
3. IT Value Estimation Issues (red)

Since all three are connected, the researcher used the following basic model as a guideline for the development of a domain specific IT Governance model.

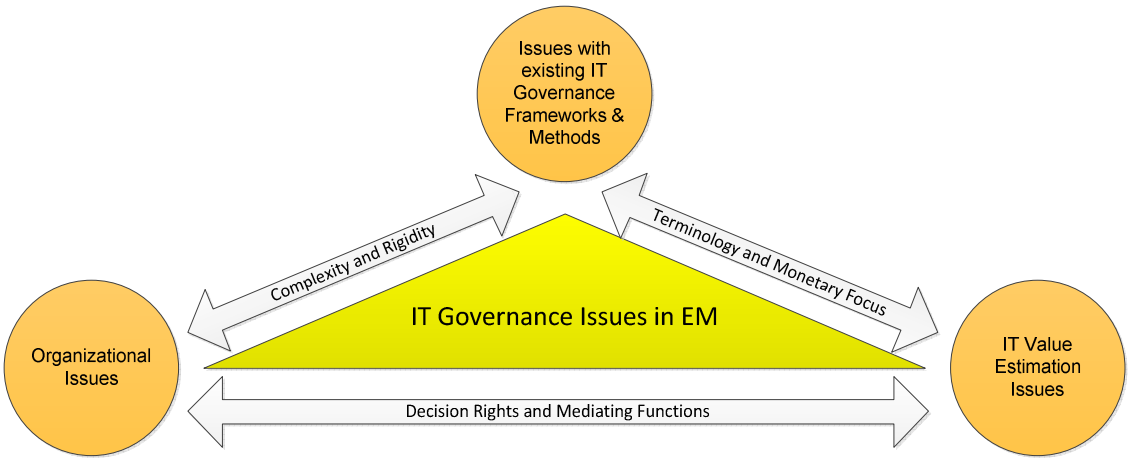


Figure 30: IT Governance Issues in EM

The three main issues are described in the following sections in more detail.

7.2.1 Issues with IT Governance Frameworks & Methods

The collected data has shown that on average only 57% of fourteen surveyed EM organizations know IT-Governance/ITSM frameworks. Whereas, the large EM organizations (seven) are all aware of these frameworks, but only 14% (one organization) of the small and medium EM organizations know them.

Most interestingly, only 21% (3 organizations) of all survey organizations think that existing frameworks are fully suitable for the EM domain.

The following chart is illustrating this finding:

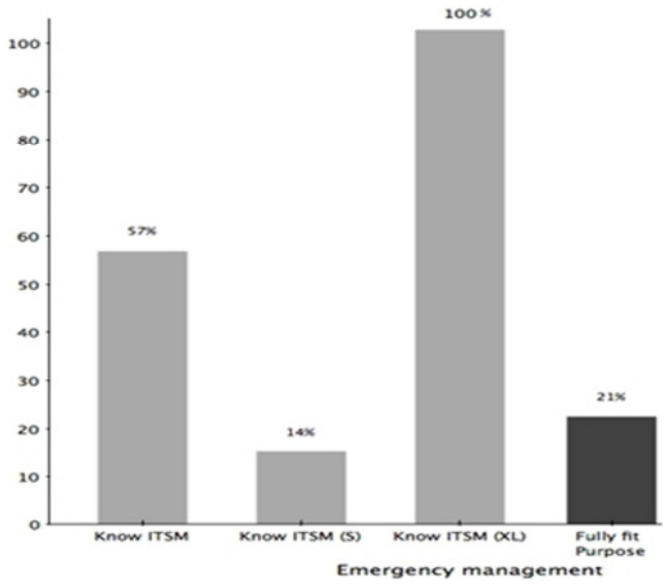


Figure 31: Awareness & Adoption of IT Governance and ITSM in EM

The following statements from experts in the field can explain these phenomena:

- “Look at the size of these publications. They are just too complex, I don’t have the time to read thousands of pages.”
- “EM is different from industry, these frameworks focus too much on monetary goals.”
- “A RACI chart is nice for steady procedures, but in emergency situations responsibilities shift depending on the escalation levels.”
- “They are not made for “Ad-hoc Teams”.”
- “It doesn’t matter if we have a maturity level of 5 if the organizations I work with don’t even know what a “maturity level” is.”

- “I’m a Fire-fighter not a Hacker, the terminology used doesn’t relate to my daily work. I would need something more tangible.”
- “We use ITIL and Cobit, because we have to by regulations – but we use it only on paper. We are first responders, we do not have time or resources to make differences between an “incident” and a “problem” – things have to work, period. Guidance on how to run IT is good, but these things need to be tailored and I don’t have the time.”
- ”I believe some of these IT governance methods are ok, but we had bad experience with other things which are not made for our purposes”
- “Yes, we use ITIL and COBIT in our organization, but not for the EM unit, the controls seem too rigid and inflexible for their purpose… so they have a special status”

Conclusively, it can be said that a large group of the interviewees see existing frameworks as too complex (at least for small and medium EM organizations). The 2011 edition of ITILv3 has 1959 pages, which is an increase of 46% compared to the initial ITILv3 version from 2007. ITIL 2011 consists of 26 main processes, more than100 sub processes, 4 functions, and over 100 roles. The exposure draft of Cobit 5.0, which will be released in 2012, has approximately 300 pages – an increase of 53% compared to Cobit 4.1 (196 pages). Cobit 5 is still work in progress, but Cobit 4.1 consists of 4 domains, 34 processes, and over 200 controlled objectives. With the integration of Val-IT and Risk-IT in Cobit 5.0 its complexity and the number of domains, processes, and controlled objectives will most likely increase as the number of pages is already indicating. Thus, it can be assumed that such volumes are not made for an entry level. Certainly, publications such as “ITIL lite”, “ITIL small scale implementation”, and “Cobit quick start” address this issue, however, other research shows that domain specific adaptation can yield even more promising results (Fry, 2010; IT Governance Institute, 2007a; Küller, et al., 2011; Taylor & Macfarlane, 2006).

Second, existing frameworks are seen as too rigid in terms of roles and responsibilities since they require rather steady organizational structures. As mentioned above, ITIL names more than 100 roles in its latest edition, which

might be appropriate for very large companies, but it is not something an EM organization can identify itself with. Decisions have to be made fast in Emergency Management situations, too many roles and different responsibilities are counterproductive. If something has to be changed fast to respond to a particular situation it is not feasible that a change request has to pass several official channels before it is acknowledged, approved, and executed. Certainly, there have to be key roles, which review decisions to ensure that all important facets have been considered but a more pragmatic solution, such as a four-eye-principle might be sufficient. Moreover, since some of the interviewees and case studies have revealed changing responsibilities (e.g. because of escalation levels), conventional RACI charts are probably not an ideal solution for every process.

Finally, most of the EM personnel cannot relate to the terminology used, and monetary driven characteristics of existing frameworks and methods. Again, this might not be a big issue in very large EM organization with a dedicated IT unit, or commercially driven organizations such as CIPs. Nevertheless, it is definitely an issue for most medium and small EM organizations, where people from the EM operations are involved in IT or even take care of the IT infrastructure. Hence, a clear relation to EM processes and EM terminology can possibly facilitate IT Governance and IT Service Management in these organizations. It has been mentioned in seminal papers of the IT Governance literature that a common (or shared) language between business and IT is important in order to align IT and business (Guldentops, 2003; Van Grembergen, et al., 2003; Weill & Ross, 2004). In the researchers perspective a shared language becomes increasingly important in special domains such and EM is. As the interviews have indicated, in EM we do not only need a common understanding about what the value of IT is to EM operations, but also a common understanding about how we can achieve it by implementing IT Governance and IT Service Management processes and methods. It was therefore the goal of this research to use EM specific terminology in all models and methods in order to increase their acceptance within this domain and facilitate the access to IT Governance and ITSM frameworks and tools. A domain specific

approach based on ITIL and COBIT is presented in Section 9.1 (ITICO4EM: A Domain Specific IT Governance Model)

7.2.2 Organizational Issues

During the data collection and analysis, the researcher found out that smaller first-responder organizations (e.g. local branches of the Red Cross, local volunteering fire-brigade) are largely unaware of their IT issues. IT Management was basically non-existent and the willingness to invest in IT was rather low. In their point of view, overarching and superordinate authorities or organizations should guide their technological progress. Typical statements of these interviewees were:

- “IT is interesting, but we don’t have the capacity”
- “We are just too small and technologies are too complex”
- “In terms of IT we have to rely on the experience of the larger fire-brigades or the academies”.

Even though these statements of the small first responders and organizations are interesting and the issues need to be addressed, the researcher had to focus on larger organizations in order to solve these problems since these small EM organizations do not have the ability or resources to tackle these problems by themselves. Improving the governance and utilization of IT in medium and large EM organizations will most likely have a positive effect on small EM organizations, if they are integrated in the medium and large organizations’ information systems and IT infrastructure.

According to the interviewees, most medium organizations had some sort of IT Management in place. However, this ranged from only a single administrator to a small IT unit. However, only one organization used process-oriented frameworks to manage their IT services and infrastructure. In this case, this was ITILv2. However, implementations were mainly focusing on to the “Helpdesk function”, “Incident Management” and “Asset Management (inventory)”. Strategic planning was, limited to the “Service Catalogue”, which was mainly driven from the IT side not from the business side. Nevertheless, the use of such a catalogue has built the basis for the communication between

IT and EM operations. In other medium organizations the cooperation between IT and EM was almost non-existent.

The large organizations surveyed had consistently a sound IT Management in place and were using IT Governance mechanisms to steer it. However, it became evident that these mechanisms were not always applied in the EM units of these organizations.

In general, it appeared that the researched Emergency Management units of municipalities, federal government, or critical-infrastructure providers are only a subset of the whole organization. As a result, most of their IT resources used in day-to-day business were managed by such mechanisms (e.g. email). However, in one case (MAC2) it became clear that as soon as technologies were solely used for emergency purposes they were deliberately excluded of this management framework. Vice versa, existing infrastructures managed by the IT unit were not used by the EM unit, because the emergency manager did not trust them. Example statements, supporting this conclusion, were:

- “Yes, EM uses IT, but nobody really cares about IT issues since the relevant processes are still paper based”
- “I think IT is just not reliable enough for our purpose in EM. How can I know that these systems are working if they have to?”
- ”Nobody feels responsible unless things don’t work and then everybody wants a say”
- “I’m pretty sure I could have designed the system. It would work in an emergency if I would know the requirements, but EM didn’t really know what they needed, so on what basis should I design it?”
- “EM gets everything they ask for! That’s not the best approach, but we do not want to put lives as stake and we just don’t know better”
- “’We are not involved unless the situation has escalated to our level…but then we have to deal with the situation…problem being is, we would need their operations and infrastructure to react effectively and efficiently, but our systems often do not fit to theirs, that’s the reason why we still have to use conventional procedures”

These statements led to the conclusion that there is a separation between IT departments and EM units. Even in state agencies, which usually have an overarching governance body, the EM units are not always fully integrated in the IT Governance processes and enterprise architecture. As a result, one can find several IT islands, which are run by the EM personnel themselves and are therefore not fully incorporated in the IT infrastructure. Moreover, existing and well-functioning IT infrastructures are not used in EM processes even though they might fulfil the requirements (e.g. reliability and availability).

In MAC2 the researcher has identified two almost similar IT infrastructures, one maintained by the IT department of the overarching agency and one maintained by the EM unit. Both were run and maintained in parallel, even though the main IT infrastructure could have been easily reused for the EM unit's purpose. On the other hand the EM unit used the agency's workflow management system for daily routines, such as expenditure claims, but they refused to use these systems in their EM processes and rely on carbon paper since they "do not trust" the system.

The only researched organization where the overarching governance body, the IT unit, and EM operations worked together relatively closely was Major Case 1. Their IT Governance structure, tries to tie the EM units and the IT department together in order to make conjoint IT decisions and to create a shared IT vision and strategy.

It can therefore be said that there is a missing link between the IT department and the operational EM unit. Hence, IT is often not aligned due to unclear responsibilities, accountabilities and missing transparency in the decision-making process. To identify how these organizations govern their IT, the researcher applied an adapted version of the decision matrix from Weill & Ross (2004). They successfully applied a similar matrix in 74 not-for profit and 168 for-profit organizations to determine the most common and (possibly most suitable) IT Governance arrangements.

The matrix shows what "archetype" is used and envisaged by IT staff and EM staff for different IT Governance related decisions. The following archetypes are used in the researcher's adapted version:

- **EM Monarchy**: Only key EM staff makes the decision
- **IT Monarchy**: Only key IT staff makes the decision
- **EM Feudal**: The EM units make independent decisions
- **Federal**: Combination of centralized decisions and EM unit / IT unit independent decisions
- **Duopoly**: Conjoint decision of IT and EM unit
- **Anarchy**: Individuals make decisions without any consultation of others

The results for the researched EM organizations are shown in the following table:

IT Gov Tasks (left-right) / IT Gov Archetypes (top-down)		Influence IT Strategy		Define IT Architecture		Maintain IT Infrastructure		Defining IT Services for Operations		IT Investments		Influence EM Strategy	
		IT	EM	IT	EM	IT	EM	IT	EM	IT	EM	IT	EM
EM Monarchy	is	0%	0%	0%	0%	0%	0%	9%	27%	0%	0%	82%	82%
	be	0%	0%	0%	0%	0%	0%	9%	73%	0%	9%	27%	64%
IT Monarchy	is	55%	64%	64%	73%	73%	64%	82%	55%	73%	73%	0%	0%
	be	18%	18%	100%	91%	91%	64%	9%	18%	0%	0%	0%	0%
EM Feudal	is	9%	0%	9%	0%	9%	9%	9%	0%	9%	9%	0%	0%
	be	0%	0%	0%	0%	9%	9%	9%	0%	0%	9%	0%	0%
Federal	is	9%	9%	18%	0%	0%	18%	0%	9%	0%	0%	0%	0%
	be	9%	18%	0%	0%	0%	18%	0%	9%	0%	0%	0%	0%
Duopoly	is	9%	9%	0%	9%	0%	0%	0%	0%	0%	9%	18%	18%
	be	73%	55%	0%	0%	0%	0%	73%	0%	100%	82%	73%	36%
Anarchy	is	18%	9%	9%	9%	18%	9%	0%	9%	18%	9%	0%	0%
	be	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
No Data / Don't know	is	0%	9%	0%	9%	0%	0%	0%	0%	0%	0%	0%	0%
	be	0%	9%	0%	9%	0%	9%	0%	0%	0%	0%	0%	0%

Table 5: How EM Governs IT

The table shows a “as-is” (red) and a “to-be” (green) situation in the surveyed EM organizations. To illustrate where the “as-is” situation is different from the “to-be” situation and where the situation is acceptable, clusters have been marked in red and green.

IT and EM staff have been asked in order to reflect the situation from different points of view. If only one perspective had been considered, the researcher could have not identified the different opinions of an “ideal archetype” between the two parties (e.g. the “to-be” archetypes in “Defining IT Services” and “Influence EM Strategy”).

As a result, the matrix revealed a couple of interesting findings:

- It shows that IT staff generally favours a “duopoly” in strategic areas (“Defining IT Services”, “Influence EM Strategy”), whereas EM staff sees themselves as the exclusive leaders and favour a “monarchy”. In the researchers perspective this reflects that EM personnel do not yet see IT as an enabler for improved EM processes but rather as a tool. However, IT personnel does see themselves as strategic partners of EM, which is indicating that it is easier for them to see the strategic value of IT initiatives to the operations. Therefore, the researcher proposes that IT should be also “Influence EM strategy” by providing information about current and future technologies, which can have an effect on EM procedures.
- A more detailed look on “Defining IT Services” lead to the conclusion, that the EM unit should define IT service requirements, but IT should negotiate the final agreement to ensure that either they can fulfil the requirements, or EM is informed that IT is not able to meet these requirements. The current situation is that in most cases the IT department just provides “standard IT services” defined by them or the day-to-day business.
- Both sides agree that IT-Strategy should be defined by EM and IT together, not only by the IT unit. In the researches view this is a good attempt to align EM and IT. However, if one is considering that EM’s is favouring a “monarchy” over a “duopoly” in the category “Influence EM Strategy”, it is also indicating that EM would rather shape the IT strategy than being shaped by IT technologies.
- Interestingly both agree that IT investments and initiatives should be decided by EM and IT even though this area is currently dominated by IT. This could be an indicator that EM and IT realize that they have to work together in order to align their interests. Together, with a “duopoly” in “IT Strategy” and “EM Strategy” a conjoint investment portfolio would be an ideal tool to serve both interests. Additionally, it would also enable a completion between “tangible” investments (such as pumps, hoses, etc.) and “intangible” investments (such as integrated databases, increased reliability of IT services, etc.).

- The only area where “as-is” and “to-be” overlap are the technological areas (IT Architecture and IT Maintenance). This was an expected outcome even though some EM personnel would like to maintain their own IT. However, this only makes sense if IT services are well defined between IT and EM, and the IT staff can deliver these IT services in an appropriate quality.

The cases studies and the interviews have also shown that there is often a significant shift regarding the responsibility and the power to direct, as soon as a crisis occurs or if the situation is escalating (see Figure 32).

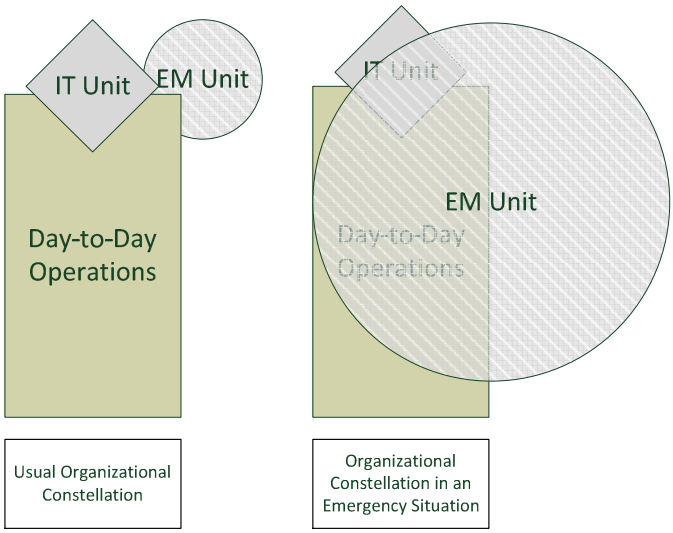


Figure 32: Responsibility shift from day-to-day operations to EM situation

In day-to-day operations of larger administrations, the EM units have often the status of an appendix. Hence, they are not involved in most decisions unless a critical situation is emerging (left side Figure 32). However, in the case of an emergency they usually take over a leading role and can supervise other units within the administration or other organizations (right side of Figure 32). Even if they have not the status of an appendix, they are often dependent on the cooperation of the day-to-day operations including their IT infrastructure and the IT unit respectively. As a result, they have to rely on IT decisions made by others - even if their requirements have not been taken into account during that decision process.

The following example (see Figure 33) will briefly illustrate how escalation levels can have an effect on the use of IT infrastructure and the information flow

between escalation levels if decisions about standards of the IT infrastructure are not made conjointly across organizations and hierarchies.

Depending on the severity of a situation, it has to be escalated to a higher EM organization (e.g. chemical plant has a leakage and the area of affect would increase). The problem is that other EM organizations, higher governmental institutions, or states do not trust IT enabled processes if they do not know the underlying IT infrastructure and their associated risks. As a result, they use “off-line” processes (e.g. carbon paper based status reports) rather than IT enabled processes.

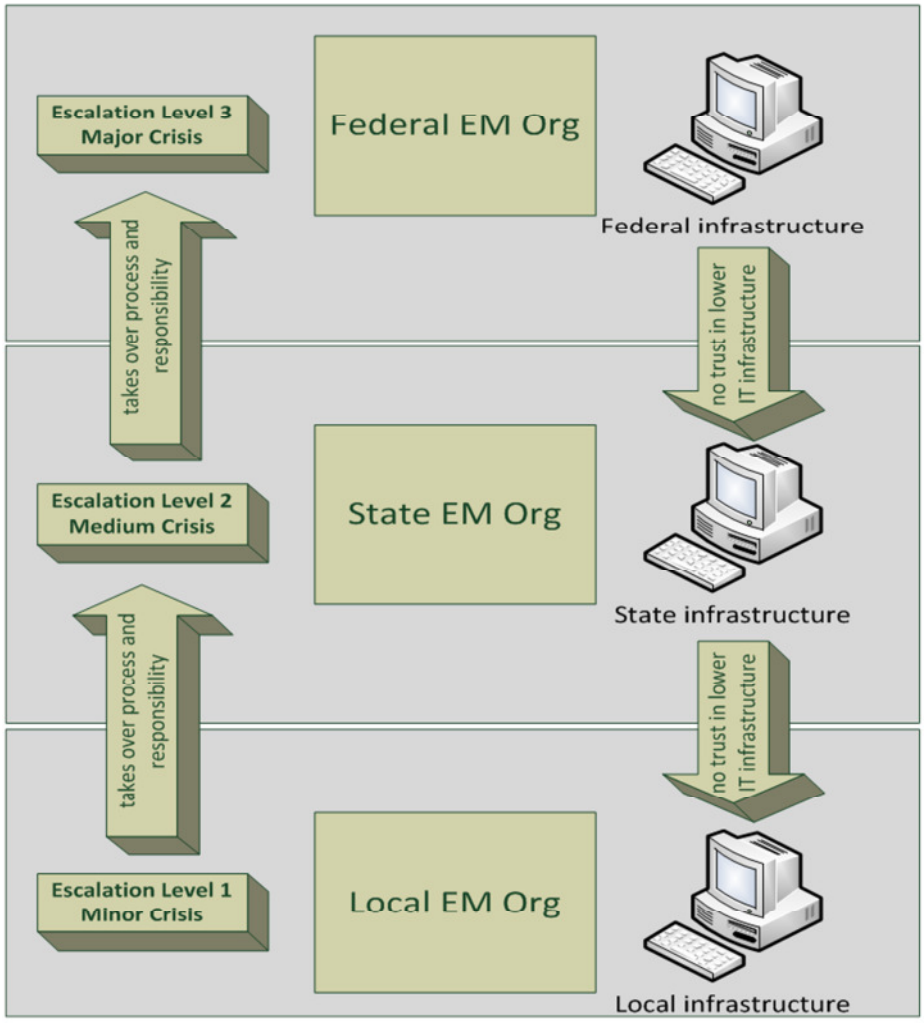


Figure 33: Escalation Levels and IT Utilizations

Consequently, the IT infrastructure and IT services do not support the operations as they should, which results in mistrust in IT enabled processes. Hence, they are using conventional methods, which are usually much slower, or they start to build their own IT infrastructure in parallel, which is often not as

effective as a holistic infrastructure and mutually defined IT services. An early integration of EM representatives in IT related decision could remedy this situation. Hence, the researcher favours new organizational approaches, which are described in Chapter 9.2 (IT-ORG / CrIO: Organizational Improvements in EM).

7.2.3 IT Value Estimation Issues

From the interviews with EM operations and IT staff it became evident that predefined emergency situations are of limited use for an IT alignment method since they cannot reflect the complexity and unpredictability of real situations. Moreover, even if all predefined emergency situations would be able to cover all eventualities, Emergency Managers are not able to realize the benefits and risks of IT for all possible situations. Consequently, it will be extremely difficult to define an IT Strategy that can be followed. Figure 34 and the following description will briefly explain why.

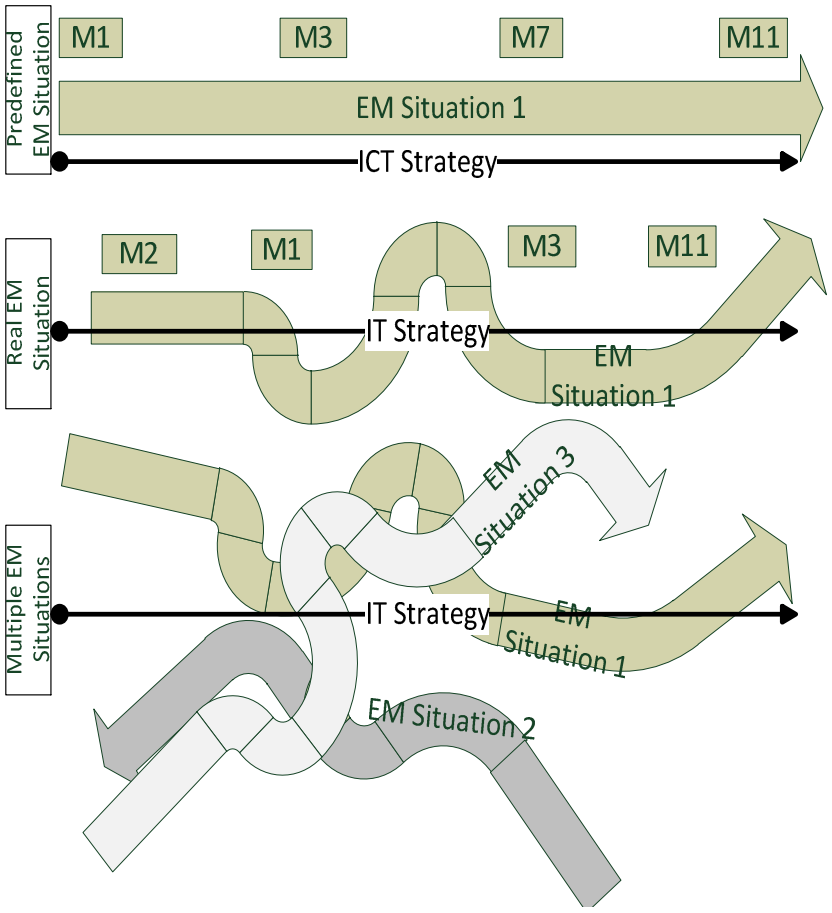


Figure 34: Scenarios vs. modular process

A “predefined EM situation” refers to a particular scenario under perfect or laboratory conditions. As one can see, a “predefined EM situation” is a straight process based on a firm set of subroutines and activities (e.g. M1, M3, M7, M11). Aligning IT with such a scenario is quite easy since we can follow well-behaved rules and have predefined goals. Therefore, “predefined EM situations” are usually straightforward. Since they are planned, it is relatively easy to create a suitable IT-strategy and identify effective and efficient IT initiatives.

In contrast, a “real EM situation” diverges from a “predefined EM situation” (e.g. different severity of impact, unexpected developments, etc.). Thus, it is quite frequent that subroutines or activities need to be shifted, skipped, or added (e.g. M1, M3, M7, M11 vs. M2, M1, M3, M11) and other IT services would be needed. As a result, the envisaged IT strategy does not fit to the current situation and becomes misaligned. The problem is that an IT strategy is quite inflexible. Short-term changes of an IT strategy are almost not possible or will have no significant effect on the current EM situation.

A slight mismatch between the IT-strategy and a real scenario is usually not too crucial. However, if we think of “multiple EM situations” and only one IT-strategy the EM/IT alignment process will be an almost impossible task since some goals and processes might compete, and the multiple possibilities cannot be anticipated. E.g., it could be the case that IT investments are “optimized” for a particular EM situation. However, in case of a different situation these IT investments could be more or less useless. In this case, IT initiatives cannot support EM processes effectively and efficiently. Consequently, we can say that it is very hard to find an IT strategy, based on planned and predefined EM situations, which can align IT initiatives to multiple and uncertain EM situations.

Nevertheless, the process analysed in the case studies have shown that most scenarios have “recurring patterns” (a set of subroutines or activities such as evacuation, search for missing people, supply water, supply shelter etc.), which can even be reused in yet unknown EM situations.

Therefore, the researcher favours a “modular IT alignment approach” based on these “recurring patterns”, instead of aligning IT to complex and predefined EM

situations. Such an alignment method, which is based on EM modules, is described in Chapter 9.3 (IVEM²: A Modular IT Value Estimation Method for EM Organizations).

8 Discussing the Data Collection and Analysis

A frequent criticism about qualitative research in general, and case studies and observations in particular, is that they do not offer enough reliability or the possibility of generalizing the conclusions drawn from the data since they are usually based on only a few cases or observations (Gable, 1994; Kerlinger & Lee, 1999; Patton, 2002; Yin, 2009). On the other hand qualitative research methods have been used successfully in IS research for years – particularly in the field of IT / IS Management (Klein & Myers, 1999; Mayring, 2000, 2002; Myers, 1997, 2008; Patton, 2002). Hence, this chapter will discuss the issues and problems during the collection and analysis phase. It will also highlight why this approach was chosen and how the researcher addressed these problems.

8.1 General issues

The goal of the data collection and analysis phase was to understand the interaction of IT and EM operations from an IT Governance perspective. Therefore, the collection of qualitative data was seen as more suitable than running statistics on a small sample group. Consequently, the researcher chose soft data over hard data and collected the needed information by interviews, case studies, and observations in order to understand the complex relation of IT in EM.

This research was based on data collected from unstructured and semi-structured interviews, cases studies of two major and four minor EM organizations, the observation of an inter-organizational emergency drill, and finally an evaluation survey. All resources, but the final evaluation survey, have been used to analyse the maturity and capability of EM organizations with regard to IT Governance. The final evaluation survey was only used to test the performance of the developed model and methods and ensure the validity of the drawn conclusions.

The first set of interviews was rather unstructured but gave the researcher a good starting point to develop a semi-structured interview with more detailed questions, and a coding scheme for the Qualitative Content Analysis (QCA)

(Mayring, 2000, 2002). The purpose of these semi-structured interviews was twofold: First, it was used to gather more data about the general issues between IT and EM, and second, it was used to collect data for the case studies. This turned out to be a very fruitful approach since it enabled the researcher to drill down into identified problems and find more evidence or to revise first assumptions. This approach goes in line with the hermeneutical research methods described in chapters 4.2.1.1 and 4.2.1.2. The NVIVO8 nodes provided in chapter 6.1.1 show the final structure of the QCA. The node development was an iterative process, which forced the researcher to revise the data and the resulting conclusions until a satisfying saturation of evidence and findings was reached, or no more examples or counter examples could be found. However, it has to be mentioned that some findings can be seen as vague or too subjective by other researchers. In these cases, the researcher found evidence of a particular problem or a fact, but was not able to find more supporting arguments in the limited set of samples. One could argue that more interviews would have been necessary to strengthen the conclusions, and the researcher cannot deny that this is true to some degree. However, the limited time frame for this research project, the lack of resources, and the difficulties to get access to other EM organizations, forced the researcher to draw a line. The decision to stop the interviews, and do not follow up these 'vague' results, was done on the basis of rationality. It was the researcher's belief that additional interviews will not reveal more significant findings, it will most probably just strengthen the already identified findings or, in the worst case, it will slightly change them. Additionally, the purpose of this research is to develop conceptual IT Governance models and tools for the EM domain. Therefore, it was decided that it would be more efficient and effective to develop basic constructs based on the given data, and discuss the refinement and application of these concepts in future research projects.

One of the major problems during the data collection phase was to get access to the right people and documents. Even though the participating organizations ensured their cooperation, it was hard to get appointments to conduct the interviews since the participants' schedules were quite tight. Furthermore, the IT-savviness was rather low of some of the interviewees, which made it difficult

to stick to the IT focus of the research. Particularly senior staff from EM operations could not relate to some of the questions (e.g. “IT Value” and “IT Decision Matrix” were terminologies that needed frequent explanation). Hence, they rather elaborated on the organizational structures and operational processes. Fortunately, the case studies were designed in a way that also IT personnel, who are usually not part of the EM operations, were interviewed by the researcher. However, it happened that their knowledge about the actual EM processes was limited. It was therefore in most cases the task of the researcher to combine the two points of view to identify the IT / EM relation, and to model the relevant processes during the analysis phase of the research.

The researcher had access to internal documents in the researched EM organizations. Unfortunately, it turned out that some of the documentation was incomplete or could not be provided due to legal restrictions and security reasons. The researcher tried to fill the missing gaps with a short Q/A either by phone, email, or in person.

The complexity of the researched domain, the lack of previous research, and the limited access to this domain demanded a multi method approach. Other researchers with a focus on quantitative research could argue that such a mixture of multiple methods would compare apples with oranges; however, the researcher argues that exactly this multi-dimensional research enabled the development of new models and tools. As shown in chapter 4.1 and specifically in chapter 4.2.1.5, consistency of findings over multiple isolated cases and different resources is a quality criterion of qualitative research, which enables a researcher to draw valid and generalizable conclusions. Particularly the case studies and observation revealed valuable insight into the processes, organizational structures, and human interactions. However, this insight would not have been given without the previous set of narrative interviews. This multiple method approach offered the researcher information richness and depth, which would not have been possible by using only one method.

In some cases the researcher had to adjust his predefined set of questions to the situation. One could argue that this would negatively influence the rigor of this research. However, already Mintzberg (1979, p. 587) states that we need richness not rigor to research organizational problems. “We uncover all kinds of

relationships in our 'hard' data, but it is only through the use of this 'soft' data that we are able to 'explain' them, and explanation is, of course, the purpose of research". Nevertheless, the rigorous documentation of the research steps was always another quality criterion during the data collection and analysis. As described above, the use of NVIVO8 as the primary research tool let the researcher file all relevant information, which was collected during the interviews and observations, and helped him to draw conclusions out of unstructured data, which was retrieved from multiple resources.

8.2 Validity, Credibility and Reliability of the Findings

The issues of validity and credibility are of concern in every research project. To address these issues during the data collection and analysis the researcher followed Mayring's (2002) 13 pillars of quality and Patton's (2002) evaluation criteria. Even though these paradigms were applied during the data collection and analysis phase in order to reduce bias, all qualitative methods are still based on the researcher's social and conceptual expertise. However, the detailed description of the cases, extracts of the interviews, and the documents in the appendix should help the reader and other researchers to follow the conclusions made, even if he or she will see things from a different angle due to the different social and scientific background. To ensure that the drawn conclusions are seen as valid by third parties, preliminary results have been shown to other researchers and experts within this field throughout the whole project. Essential assumptions and theories have been discussed on a frequent level. Some of the results have also been published and peer-reviewed at renowned international conferences. Even though this cannot eliminate all eventualities, it indicates that the researcher's findings are comprehensible, transparent, and reasonable.

To demonstrate the generalizability of the research results, a final 'evaluation survey' was conducted to measure the effectiveness and efficiency of the resulting conceptual IT Governance models and tools by comparing them to existing processes and methods.

Regarding the reliability, the researcher doubts that his results will be 100% reproducible if the project would be repeated today. Organizations and people evolve; moreover, a generation shift was realized within this domain. The new generation of decision makers grew up with the ubiquity of IT. Hence, the perception of IT for their work will increase. Furthermore, if the project would be conducted in the same participating organizations, the researcher believes that the overall IT Governance maturity in these organizations has increased since the participants were confronted with the question: 'How does IT affect my work and how can IT be governed to increase its value to me?' Therefore, the trustworthiness of this research is only based upon the validity and credibility.

8.3 Ethical Considerations

Since human participants were involved in the research, the University's ethical code had to be applied. Even though only adult professionals have been interviewed, the questions asked had to be approved by the University's ethics committee, this turned out to be a hurdle in the beginning since the research method was based upon unstructured and narrative interviews and semi-structured interviews. Luckily, in a second amendment form an expanded questionnaire was approved, which included a very broad question in the section "Other Questions" that enabled the researcher to include "ad-hoc" questions during the interviews.

Another ethical obligation by the University was to anonymize the interviews, so nobody could be harassed or punished based on his or her statements. Additionally, some of the organizations only agreed to participate in this research if the author would sign a non-disclosure agreement. Hence, all relevant and cited interview sections were anonymized and in some cases rewritten so that no one can identify an interviewee based on his statements or speaking patterns. As a positive fact, this reduced the effort to transcribe the whole interviews and increased readability. As a negative fact, it might reduce the transparency and validity of the collected data in other researchers' view. However, since not the person's name was in the focus of this research but rather his or her expertise about EM / IT processes, it is the author's view that this should not make this research less trustworthy. To ensure that the

statements and interviewee selection was reasonable and relevant, demographic data about the participants had been filed.

PART IV:
Conceptual Models & Methods

9 Improving IT Governance and Strategic IT Alignment in EM

Previous research has identified that IT Governance frameworks and methods are used in individual ways since different organizations have diverse motivations and needs. One way to tackle this problem is to build metamodels and identify recurring patterns, which lead to a better understanding of causes and effects (Looso & Goeken, 2010).

In order to build a domain specific IT Governance method the researcher had to get to know the domain's needs, identify their barriers, and follow a suitable engineering approach, which is based on Bjorner's (2010) and Naumann's (2007) domain engineering methods. The engineering process used to design an IT Governance reference model for the EM domain is shown in the following figure:

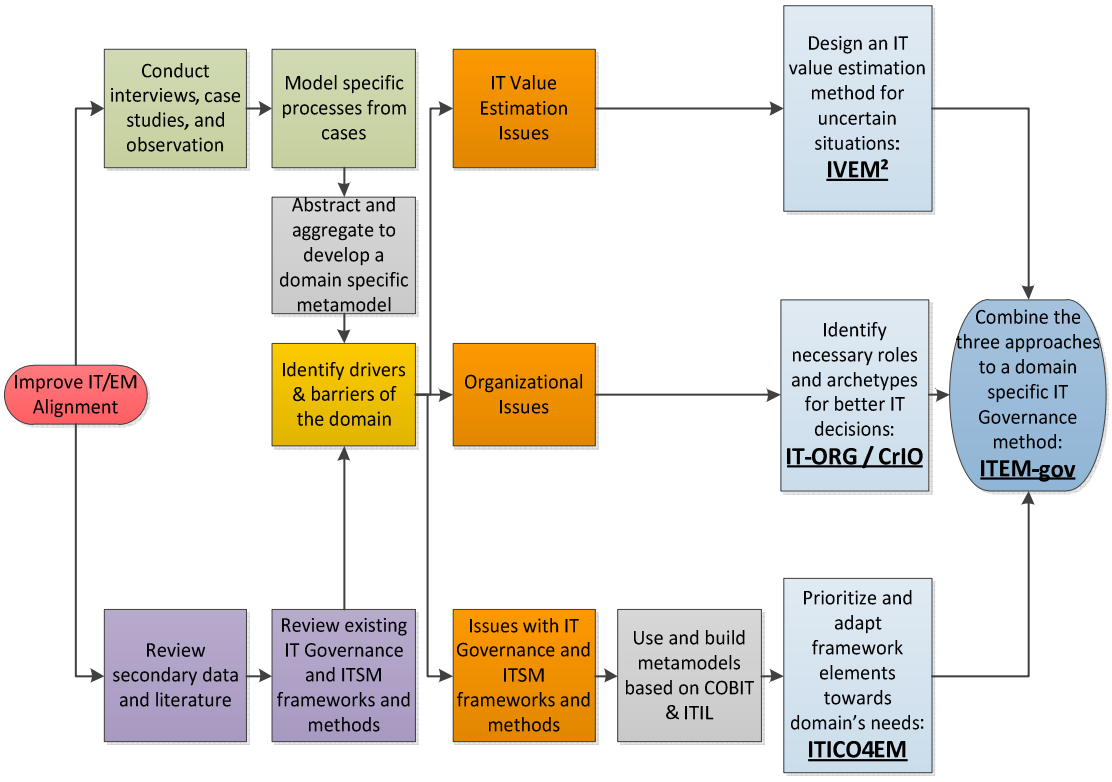


Figure 35: Engineering Process of a EM Domain Specific IT Governance Method

The following sections will describe the development of the three approaches (light blue):

ITICO4EM: A simplification and adaptation of existing IT Governance and ITSM frameworks. The adaptations were made to address the EM specific need and to provide guidelines, which are also usable by small and medium organizations, which do not have the capacities to implement ITIL and COBIT.

IT-ORG / CrIO: Identification of necessary roles and archetypes for better IT decisions and the creation of a shared IT vision of all stakeholders in EM processes.

IVEM²: A modular IT value estimation method for EM organizations, which should enable decision makers in EM to estimate the impact and risk of IT initiatives even in uncertain environments and consequently build a prioritized IT portfolio.

Finally, the three approaches are combined into an IT Governance Reference Model for EM Organizations (dark blue: **ITEM-gov**).

Combining the three approaches will therefore address the issues identified in Chapter 7.2 as shown in the following figure:

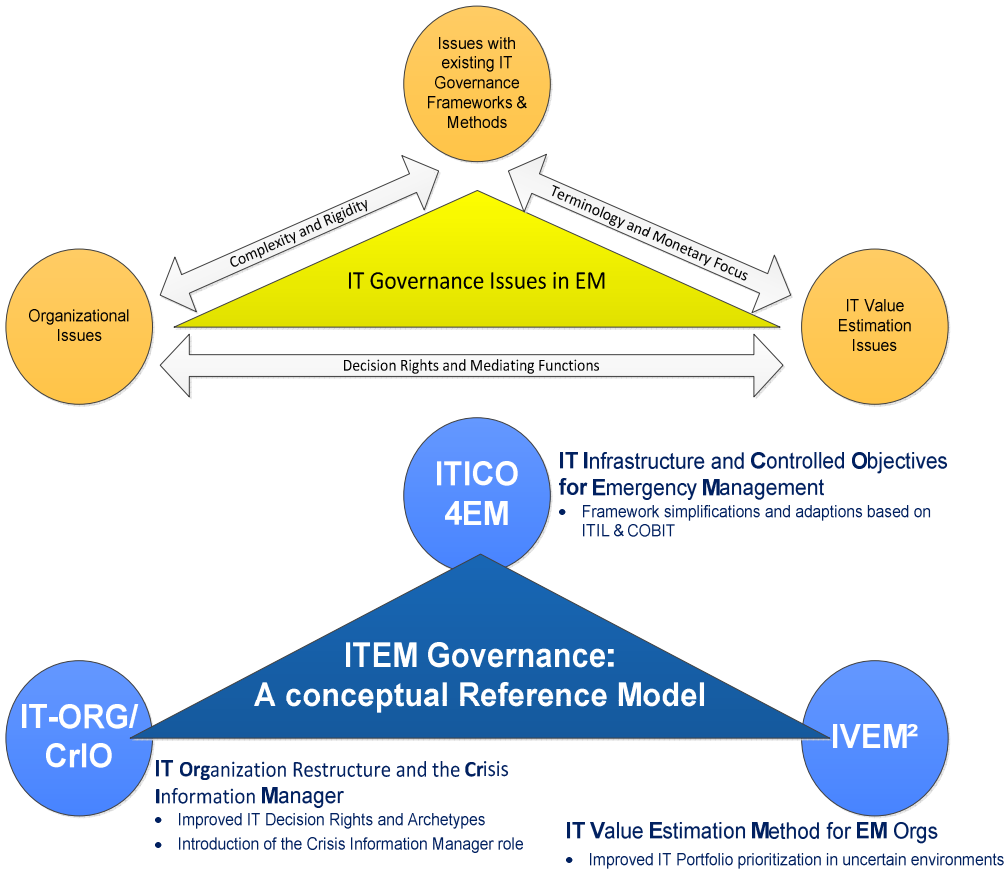


Figure 36: ITEM Overview based on ITICO4EM, IT-ORG / CrIO, IVEM²

9.1 ITICO4EM: A Domain Specific IT Governance Model

In Chapter 7.2.1 the general issues of the EM domain with IT Governance and ITSM frameworks were identified. The researcher tried to identify why these frameworks are not fully accepted and applied in the researched EM organizations. Moreover, from the interviews and case studies, it became clear that there is no single framework that could be applied to all phases of an emergency since these stages differ largely in terms of their processes and timelines. Therefore, it had to be identified which of these frameworks are the most fruitful in the EM domain. Hence, the following table shows the most common IT Governance frameworks and IT value methods in relation to the four phases of Emergency Management.

Phases	Goals	Frameworks	Issues
Prevention	Define strategic goals	Weil/Ross decision matrix	often not suitable for "not-for-profit" organizations
	Show ICT value and risks	COBIT	
	Establish clear responsibilities	Val-IT	
	Optimize ICT portfolio towards different scenarios	Risk-IT	not designed for EM organization structures
	Build a sound and sustainable enterprise architecture	ITIL/ITSM	
	Learn from previous disaster and review ICT strategy	CMM	
		BSC, BVIT, CVE, etc.	cannot cope with ad-hoc teams
		ROI, NPV, etc.	
Preparation	Prepare for the inevitable	COBIT	cannot cope with "uncertain situations"
	Be flexible to severity of impact	BS25999 (BCM)	
	Build a sound ICT environment to support EM operations	ITIL/ITSM	give only rough guidelines, to complex to adapt to EM
Response	Keep "IT" running	ITIL/ITSM	
	Support EM operations		
Recovery	Recover damaged IT infrastructure quickly	ITIL/ITSM	not designed for multi-organizational procedures

Table 6: IT Governance / ITSM Frameworks and EM Phases

As one can see by the number of applicable frameworks and methods, the most suitable phases for strategic IT decisions are prevention & preparation since they are prior to the impact. Therefore, this research is concentrated on these phases. However, due to time and budget constraints this research did not investigate all of the identified frameworks. Thus, only the most common and promising were picked and analysed. In this case, the decision fell on COBIT and ITIL. Besides these two “standard frameworks”, also VAL IT and RISK IT have been considered. However, since they are strongly connected to COBIT they were not completely used. Nevertheless, they had some influence

in the design phase of IVEM² (see Chapter 9.3). Therefore, the following chapters will describe the development of domain specific IT Governance and ITSM processes based on existing frameworks.

It is not the intention of this research to develop a complete new IT Governance or ITSM framework, it is rather envisaged to create a customized subset of these frameworks for the EM domain and make adaptations where needed. This will lower the barriers to implement IT Governance / ITSM processes and structures, but leaves the EM organizations the opportunity to upgrade to more detailed ITIL or COBIT implementations without changing their whole procedures. Additionally, the close relation to ITIL and COBIT will enable EM organizations, which have already implemented or are in the process of implementing one of these frameworks, to adapt (or at least review) their processes by using ITICO4EM as a reference model.

The following requirements have been identified and used for the development of a domain specific set of IT Governance and ITSM procedures:

- High flexibility, to react to uncertain situations
- High reliability of systems and changes
- Improved integration of systems within and across organizations
- Solutions must be in line with limited resources
- Quick and easy reporting
- Reduction of complexity
- Use of EM specific terminology

9.1.1 Metamodeling of Existing Frameworks to Identify Reusable Items

ITIL and COBIT metamodels, as well as framework mappings, were reused from previous research projects and publications (Goeken & Alter, 2008, 2009; Goeken, et al., 2009; IT Service Management Forum, 2008; Looso & Goeken, 2010). For this research, the metamodeling approach is used in the sense of “model of a model” or “macro-level-design” not as “modelling language description” or “micro-level-design” (Karagiannis & Hoefferer, 2006) and follows Rolland’s (1993) abstraction layers as described in Chapter 4.2.2.1.

Goeken et al. have used conceptual metamodels to represent existing IT Governance and ITSM frameworks on an abstract level. Such an abstraction can help to analyse existing frameworks in order to demonstrate ways to improve them or adapt them according to the specific needs of an enterprise or an industry. Consequently, the researcher has used this technique to develop a domain specific IT Governance / IT Service Management framework. The following figures illustrate the meta-level of IT Governance processes from COBIT and ITIL.

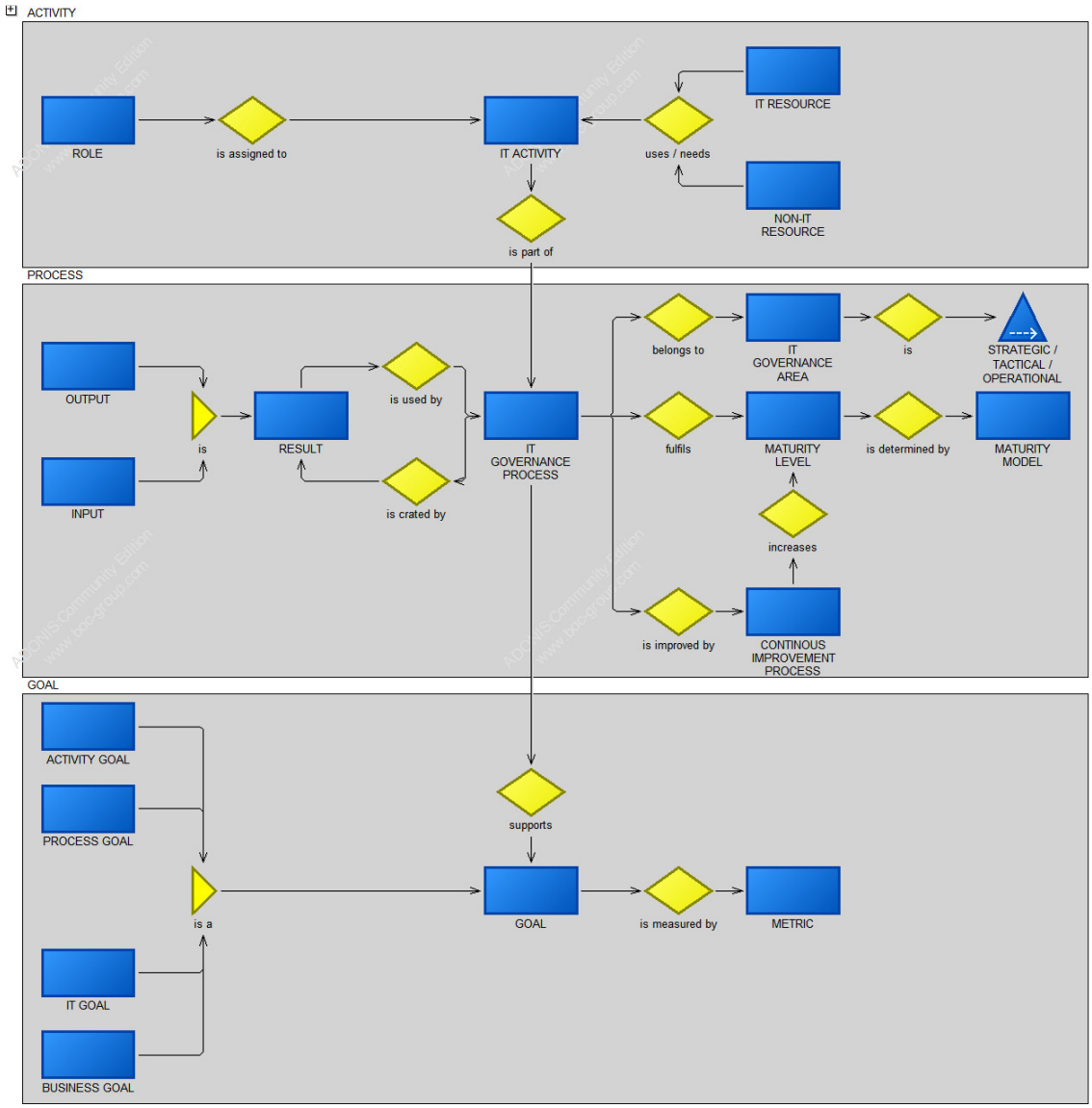


Figure 37: IT Governance Processes - Meta-Level of COBIT & ITIL (based on Goeken & Alter, 2008; Goeken, et al., 2009)

The metamodel demonstrates that both frameworks follow the same structure on the process level. Hence, this metamodel of IT Governance processes was

used as a reference for the ITICO4EM processes. Implementing the same IT Governance process structure ensures that all ITICO4EM processes are compatible with COBIT and ITIL. Consequently, EM organizations are able to replace or refine process if necessary without having to rethink the general structure.

Even though Figure 37 shows that ITIL and COBIT have similarities on the process layer, the metamodel does not reveal in which IT Governance areas ITIL and COBIT processes overlap and which of these processes is relevant for EM organizations. However, in order to develop ITICO4EM it was necessary to map relevant IT Governance processes to EM's needs.

For this purpose, the researcher used an ITIL / COBIT mapping from the IT Governance Institute as a basis. The first step was to identify their main processes and functions, which overlap, and then to summarize and aggregate them in a meta-process map, which is shown in the following figure (IT Governance Institute, 2008b; IT Service Management Forum, 2008, 2009a).

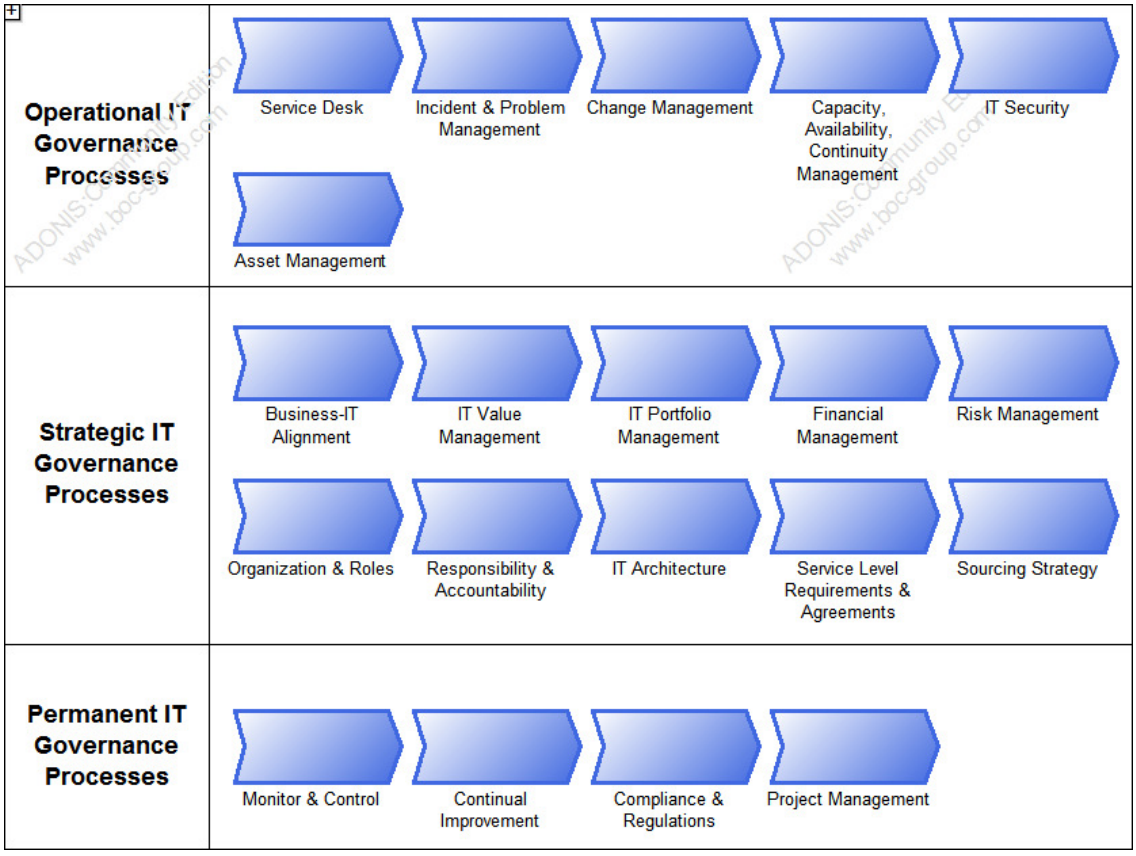


Figure 38: COBIT / ITIL Meta-Process Map

The meta-process map gave the researcher a good guideline about which core processes of the two leading IT Governance frameworks (ITIL & COBIT) are essential for the development of a domain specific process structure. The metamodel in Figure 38 shows that three main process levels were identified to which both frameworks can relate (Operational / Strategic / Permanent). It also shows the core processes of each level.

Since, a meta-model can only describe a certain aspect the guiding idea of this meta-process map was to simplify and unify these frameworks. It therefore shows aggregated processes and process layers. In further steps, the metamodel was used to derive the most promising sub-processes of existing frameworks and combine them to the ITICO4EM approach. This selection approach is explained in the following chapter.

9.1.2 Identifying Reusable Processes from Existing Frameworks

By using the metamodel of COBIT and ITIL the researcher as able to identify which processes and controlled objectives can be reused, must be altered, or are of lesser importance to the EM domain. To reduce complexity of the frameworks and generate a domain specific method, the researcher followed Fry's (2011, p. 17) methodology to filter relevant processes and control objectives by using the following steps as shown in Figure 39.

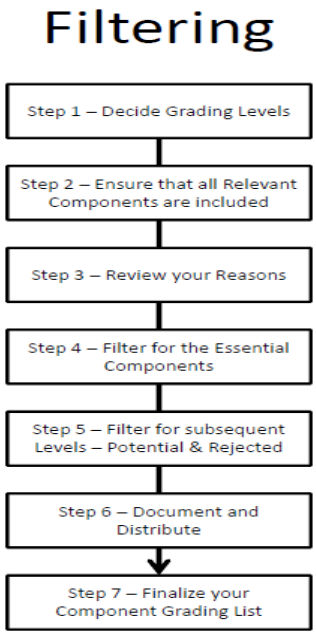


Figure 39: Filtering Process for ITIL & COBIT

9.1.2.1 Reusable ITIL Processes

With regard to operational IT Governance processes (see meta-process map Figure 38, p.178), ITILv3 was used as the leading framework for this research. Hence, ITIL processes have been reviewed according to their applicability in EM organizations. To meet the special requirement “reduce complexity”, ITIL ‘lite’ or “small-scale“ processes (see Figure 39 and Figure 40) were used as a guideline, however, in some cases the research felt that these short versions of ITIL were too shallow. Consequently, the full-scale version of ITIL was used for completion (Fry, 2010, 2011; Taylor & Macfarlane, 2006). The processes are separated into four categories (action components, influencing components, resourcing components, underpinning components), from which applicable processes from the ITIL Books (service strategy, service design, service transition, service operations, and continual service improvement) can be chosen.

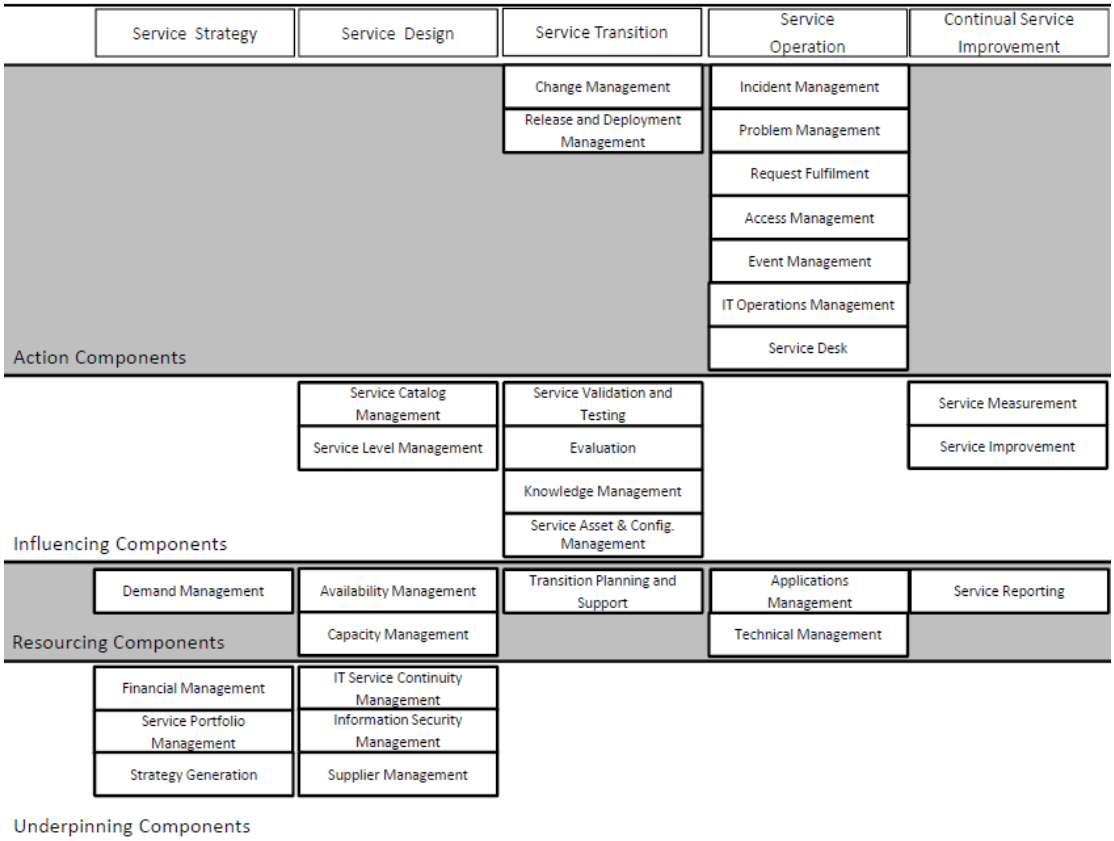


Figure 40: ITIL 'lite' processes (Fry, 2011, p. 20)

- *Action components*: They require actions of an operational nature to be performed as part of their normal operation

- *Influence Components*: These components influence the way that Action Components perform
- *Resource Components*: They ensure that all other components have the resources to deliver quality services
- *Underpinning Components*: These processes provide the support required by all other components (e.g. Finance).

The following ITIL processes have been identified as the most promising for a EM specific IT Governance framework:

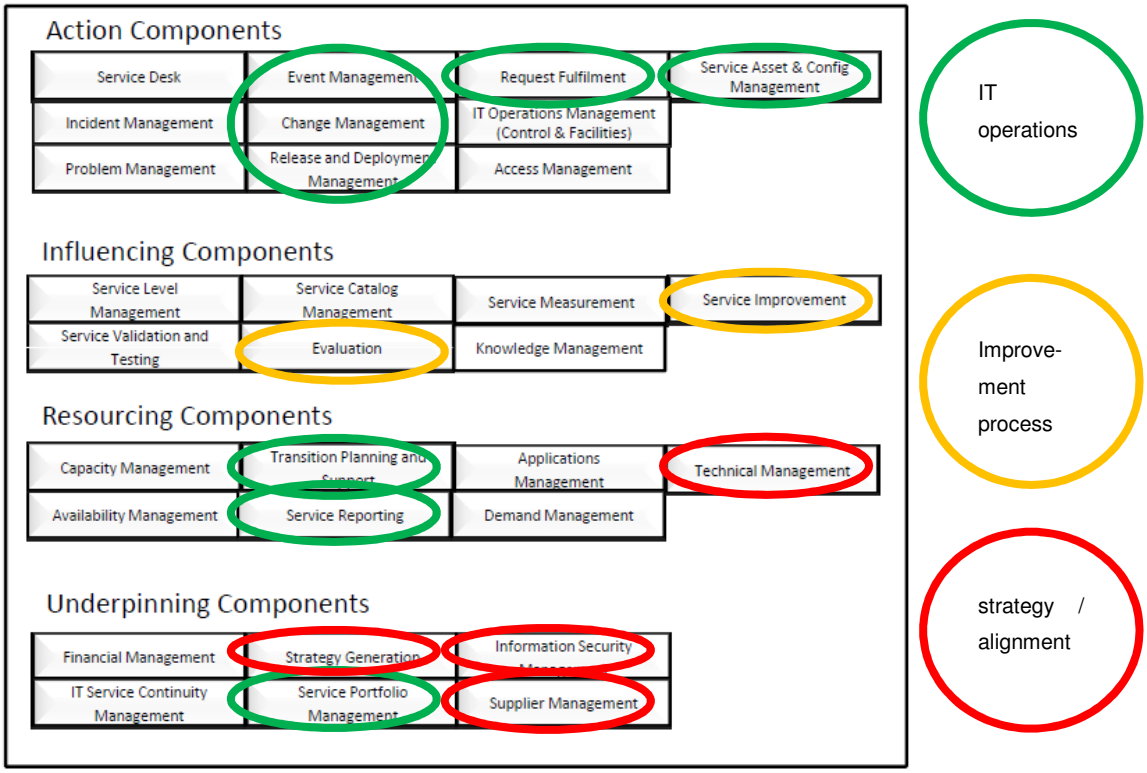


Figure 41: ITIL Processes for EM organizatons, adapted from (Fry, 2011, p. 15)

The “IT operations processes” (see green circles in Figure 41) have been chosen to support EM organizations during all emergency phases. Well-functioning IT infrastructures are essential to EM operations in every stage of an emergency. Hence, the used IT services have to meet the agreed service levels; otherwise, the use of IT enabled processes would put lives at stake. A reliable and transparent IT infrastructure and quality IT services generate trust amongst EM operations personnel. The interviews have shown that, due to the lack of transparent IT Service operation processes, EM personnel do not rely on technology in crisis situations, they rather use slower and often less precise

analogue services or manual processes (e.g. carbon paper and human couriers to distribute reports) instead of digital solutions (e.g. digital documents and automated workflow systems). The increased trust in IT services will most likely affect the willingness to invest in more advanced technologies, vice versa, a fragile IT infrastructure will only encourage IT reluctance. As a result, EM operations will miss opportunities to improve their processes.

“Improvement processes” (see yellow circles in Figure 41) were chosen because business processes and technologies change quite rapidly today. Hence, new opportunities and risks will emerge. The continual service and process improvement ensures cost-efficient and trouble-free IT operations. Improved IT services can even enable new processes, because they might be able to fulfil the high requirements of EM operations.

As a third component, “strategy / alignment elements” (see red circles in Figure 41) were chosen to ensure the alignment of IT services and technologies. “Demand Management” and “Strategy Generation” define the services and technological directions to support EM operations. Without these components, a proficient IT Service Portfolio would not be feasible. Moreover, investments in wrong technologies will waste the limited resources of EM organizations, therefore it is necessary for EM organizations to know about the value of IT towards their operations and subsequently manage their finances and make the ‘right’ investments.

9.1.2.2 Reusable COBIT Processes

COBIT is the second pillar for the design of ITICO4EM and mainly influenced the selection of the strategic IT Governance processes (see meta-process map Figure 38, p.178). Consequently, the COBIT 4.1 framework, or respectively it’s derivation “COBIT QuickStart 2nd Edt.” have been reviewed to identify suitable and applicable processes for the EM domain. To keep the complexity of ITICO4EM within limits the researcher has used mainly COBIT QuickStart as a reference, but has also used processes and controls of COBIT 4.1 whenever it was necessary to add more depth. COBIT QuickStart was mainly designed for small and medium enterprises (SME) or organizations with low IT utilization. However, it can also be used as a starting point for organisations who are

dealing with IT Governance for the first time. In contrast to COBIT 4.1 with four domains, 34 processes, and 210 controlled objectives, COBIT QuickStart 2nd Edt. consists of only 59 control objectives and 32 processes in four domains (IT Governance Institute, 2007a, 2007b). The following figure will give an overview about the COBIT processes used in ITICO4EM (IT Governance Institute, 2007a).

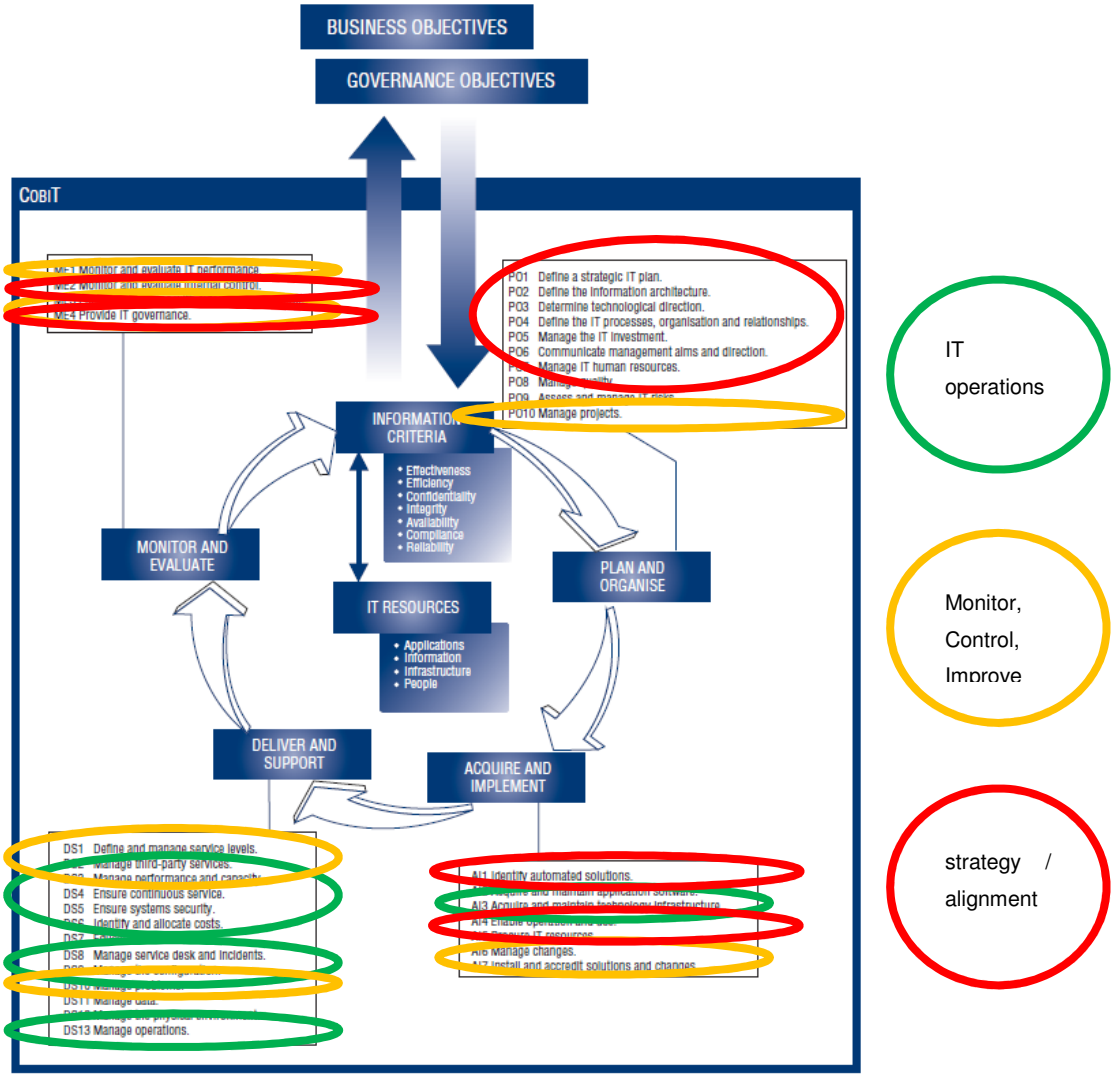


Figure 42: COBIT processes used in ITICO4EM (cp. IT Governance Institute, 2007a, p. 10)

Sub processes and controls have been used from the following main processes:

- PO1 Define a strategic plan
- PO2 Define technological architecture
- PO3 Define technological direction

- PO4 Define IT processes, organization and relationships
- PO5 Manage the IT investment
- PO8 Manage Quality
- PO9 Assess and manage IT risks
- PO10 Manage Projects
- AI1 Identify automated solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure
- AI5 Procure IT resources
- AI6 Manage changes
- AI7 Install and accredit solutions and changes,
- DS1 Define and manage service levels
- DS2 Manage third party services
- DS3 Manage performance and capacity
- DS4 Manage continuous service
- DS5 Manage systems security
- DS8 Manage service desk and incidents
- DS9 Manage the configuration
- DS10 Manage problems
- DS11 Manage data
- DS12 Manage the physical environment
- DS13 Manage operations
- ME1 Monitor and evaluate IT performance
- ME3 Ensure compliance
- ME4 Provide IT Governance

Of course, not all sub-processes and controls of these 28 main processes have been used in ITICO4EM. A full mapping can be found in the appendix.

9.1.3 Adapting and Redesigning IT Governance Processes for EM Organizations

The lack of appropriate frameworks was confirmed by almost all of the interviewees (cp. Figure 31, p.153). However, the existing frameworks have

promising approaches, which can be used as a basis for EM organizations. Probably some of the methods can partially be applied to the domain of Emergency Management, but researchers and emergency managers jointly agree that conventional techniques can usually not be applied without adaptation (Di Maio, 2003a, 2003b; Dwarkanath & Dakonta, 2006; Iannella & Henricksen, 2007; Iannella, et al., 2007; Küller, et al., 2011; Sethibe, et al., 2007; Van Den Eede & Van de Walle, 2005; Vogt & Hales, 2010).

9.1.3.1 ITICO4EM – ITIL – COBIT Mapping

To adapt these frameworks and develop a domain specific version, the researcher had to map, combine, and aggregate identified framework elements. The ITICO4EM processes have been derived from ITIL and COBIT, hence they are based on proven frameworks. This mapping process was done by using a simple table, which was iteratively refined with participating organizations until a satisfactory level was reached.

In addition, the ITICO4EM mapping gives the EM organizations the possibility to "look deeper" into some processes if needed since it uses the official ITIL and COBIT process numbers (E.g. SS 2.1 for ITIL Service Strategy Book, Process 2.1). The following snippet of this table (Table 7) is shown as an example; the full table can be found in Appendix F (ITCO4EM-ITIL-COBIT Mapping).

	SL-1.4 Identify operation's needs SL-2.1 Identify the value of IT towards recurring processes and/or scenarios SL-2.2 Align IT initiatives with your strategic goals using information about their value, risks and costs and build a prioritized IT portfolio SL-2.3 Ensure balance, -long-term value and reusability of IT initiatives	SS-4.2 Develop the offerings SS-4.4 Prepare for execution SS-5.1 Financial management SS-5.2 Return on investment SS-5.3 Service portfolio management SS-5.4 Service portfolio management methods SS-5.5 Demand Management SS-6.5 Sourcing strategy SS-7.2 Strategy and design SS-7.3 Strategy and transition SS-7.4 Strategy and operations SS-9.3 Preserving value SD-3.4 Identifying and documenting business requirements and drivers SD-8.1 Business impact analysis	PO-5.4 Cost management PO-5.5 Benefit management PO-8.4 Customer focus ME-4.1 Establishment of an IT governance framework ME-4.2 Strategic Alignment ME-4.3 Value delivery ME-4.4 Resource management
esponsibilities on Rights	SL-3.1 Involve EM operations in IT decisions to ensure strategic alignment SL-3.2 Involve IT in EM process design to ensure efficient and effective process support SL-3.3 Implement a Crisis Information Officer (CrIO) who co-ordinates between IT initiatives and EM operations and supervises strategic, tactic, and operational goals SL-3.4 Implement an IT governance board to steer IT initiatives and strategic directions from an EM perspective SL-4.1 Consider shifting organizational structures and decision rights. Ensure that all possible "process owners" are involved in decisions about the design and service levels requirements of IT initiatives SL-4.2 Establish inter-organizational IT co-ordination committees to streamline inter-organizational processes and optimize IT services and infrastructures for a robust, effective and efficient information flows	SS-2.6 Functions across the lifecycle SS-6.1 Organizational development SS-6.3 Organizational design SS-6.4 Organizational culture SS-6.5 Sourcing strategy SD-2.3 Functions and processes across the lifecycle SD-6.1 Functional roles analysis SD-6.4 Roles and Responsibilities ST-6.1 Generic roles ST-6.3 Organizational models to support service transition SO-2.3 Functions across the lifecycle SO-3.1 Functions, groups, teams, departments and divisions SO-3.2 Reactive vs. proactive organizations	RACI Process Controls (PC2, PC3, -P4) PO-3.5 IT architecture board PO-4.2 IT strategy committee PO-4.3 IT steering committee PO-4.4 Organizational placement of the IT function PO-4.5 IT organizational structure PO-4.6 Establishment of roles and responsibilities PO-4.7 Responsibility for IT quality PO-4.8 Responsibility for risk, security and compliance PO-4.9 Data and system ownership DS-4.7 Distribution of the IT continuity plan

Table 7: ITICO4EM - ITIL - COBIT Mapping (snippet)

As one can see in the table, the processes have been mapped according to their level (strategic, operational, and permanent) and the EM phase (prevention, preparation, response, and recovery). From this mapping the researcher developed the main ITICO4EM processes, and finally identified, combined, aggregated, and altered processes that are more detailed. As result of this mapping process, the researcher developed a model to visualize how these processes are connected. The proposed simplified IT Governance model is shown in the following figure.

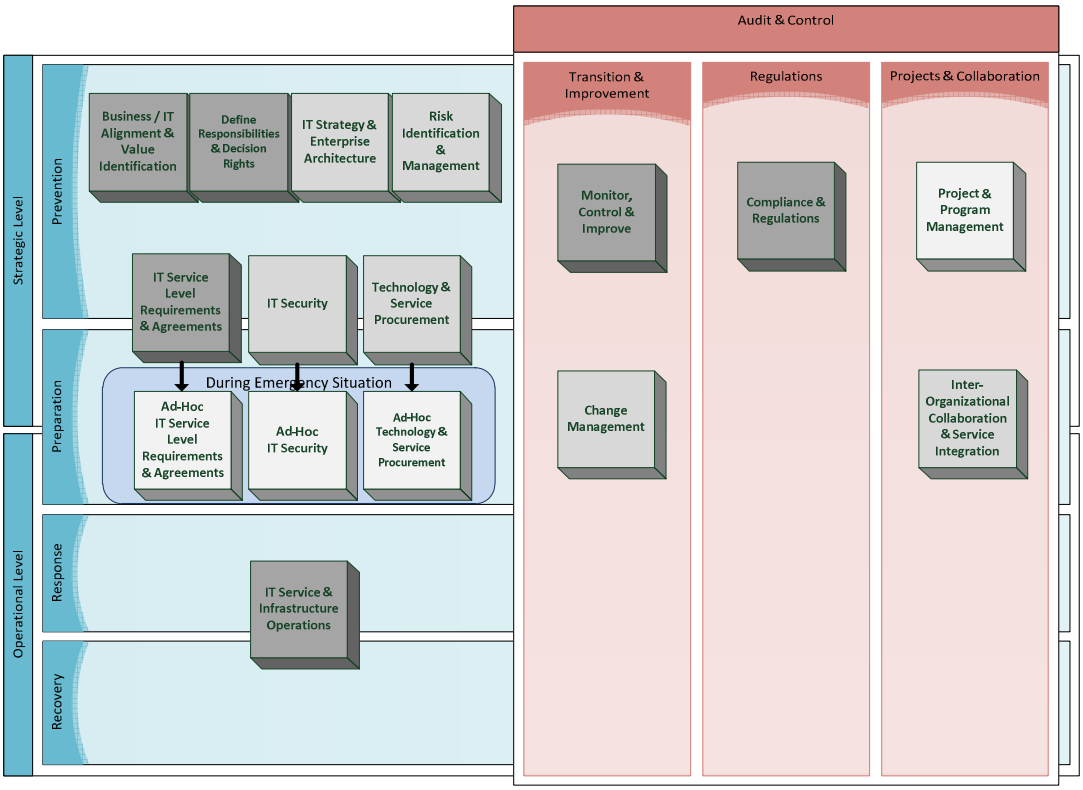


Figure 43: ITICO4EM a simplified IT Governance & IT Service Management Model

Compared to ITIL and COBIT process maps, ITICO4EM is rather simple and clean. The model is based on the three main IT Governance levels, which have been identified in the meta-process map (see Figure 38, p.178): Strategic Level, Operational Level, and Audit & Control. It also features the four emergency phases (Prevention, Preparation, Response, and Recovery) in order to represent the relevance to the EM domain. The model consists of six "core processes" (dark grey) with 36 sub-processes and 10 discretionary processes (medium and light grey) with 43 sub-processes.

The model is based on horizontal (blue) and vertical (red) layers. The horizontal layers represent the separation between strategic and operational processes. Only the “ad-hoc” sub-processes and their parent elements cannot be assigned clearly, since they have strategic and operational origins. The “IT service and infrastructure operations” are operational but are used in two EM phases. Hence, it is represented as an overlapping element between the two EM layers. The vertical layer represents permanent or frequently recurring IT Governance processes. They cannot be assigned to a particular EM phase and usually have strategic and operational characteristics.

The boxes in this model represent the main IT Governance processes of ITICO4EM. The different colours represent their importance: Dark grey boxes are mandatory to ensure at least basic IT Governance structures, medium to light grey boxes are discretionary but can improve the IT Governance performance of EM organizations. The main processes and implementation recommendations are described in in the following sections.

9.1.3.2 ITICO4EM Process Descriptions

The ITICO4EM model is composed of 16 main processes in total, which are split into “core processes” (dark grey), “optional processes” (medium grey), and “ad-hoc processes” (light grey). Each of these main processes represents a group of sub-processes. The following descriptions will give a brief overview of these main processes. A detailed list and description of the sub-processes can be found in Appendix G (ITCO4EM – Detailed Processes), of which a snippet is shown in the following figure:

ProcessLevel	EMPhase	ITICO4EMProcesses	ITICO4EMDetailed-Processes---Explanation
Strategic Level	Prevention	Business-/-IT-Alignment-&-Value-Identification	**SL-0.1-Establish-a-mindset-of-"IT-as-an-enabler"-for-EM-services** --Before-applying-IT-governance-methods-EM-organizations-have-to-establish-an-understanding-of-"IT-as-an-enabler"-in-technical-and-non-technical-units.-It-has-to-be-understood-by-non-technical-EM-units-that-IT-is-not--a-cryptic-and--unreliable-technology-but-can-provide-fundamental-support-and-opportunities-for-EM-processes.-On-the-other-hand-technical-units-have-to-understand-that-IT-is-not-there-because-EM-wants-new-technology,-IT-is-there-because-EM-wants-to-improve-their-EM-processes.
			SL-0.2-Foster-to--think-in-IT-services-rather-than-IT-technology --Shift-from-a-technological-point-of-view-to-a-service-oriented-point-of-view.-An-IT-service-can-be-understood-and-evaluated-by-technical-staff-as-well-as-non-technical-staff.-the-main-goal-is-to-realize-the-value-of-IT-to--the-EM-process.
			SL-0.3-Establish-a-transparent-IT-governance-which-enables-EM-operations-to-steer-and-therefore-trust-IT --IT-initiatives-should-become-clear-to--non-technical-steering-committee-members.-It-is-essential-that-IT-decisions-on-a-high-level-(e.g.-on-project,-programme,-and-portfolio)-involve-non-technical-members-to-increase-the-acceptance-of-IT-supported-and-improved-EM-processes.-Risks-and-opportunities-of-IT-initiatives-have-to-be-presented-in-non-technical-vocabulary-to-make-their-impact-on-the-operational-processes-more-transparent.
			SL-1.1-Define-and-document-strategic-goals-of-the-organization --It-is-important-to-define-and-document-the-strategic-goals-of-an-EM-organization-in-order-to-align-IT-initiatives-towards-them.-Documented-strategic-goals-can-be-assed-and-prioritized-according-to-their-impact.
			SL-1.2-Identify-threatening-scenarios-and-their-likelihood --Every-EM-organization-has-a-different-set-and-likelihood-of-possible--threatening-scenarios-(e.g.-tsunamis-are-only-of-concern-to-EM-organizations-along-the-coast-line,-and-the-likelihood-of-tsunamis-varies-in-different-coastal-regions).-Knowing-possible-scenarios-and-their-likelihood-will-help-to-develop-the-most-suitable-countermeasures.

Figure 44: ITICO4EM Detailed Processes Description (Snippet)

The table “ITICO4EM Detailed-Processes” gives EM organizations concise explanations about each process. It uses EM related terminologies to help EM staff to understand the relation between the IT Governance process and their work. The processes descriptions are not elaborate but EM staff with a bit of IT knowledge should be able to understand the general aim of the processes. If more information is needed, one can directly lookup the associated ITIL and COBIT processes using the ITICO4EM mapping. The following paragraphs will briefly describe the major goals of the main processes.

Core Processes

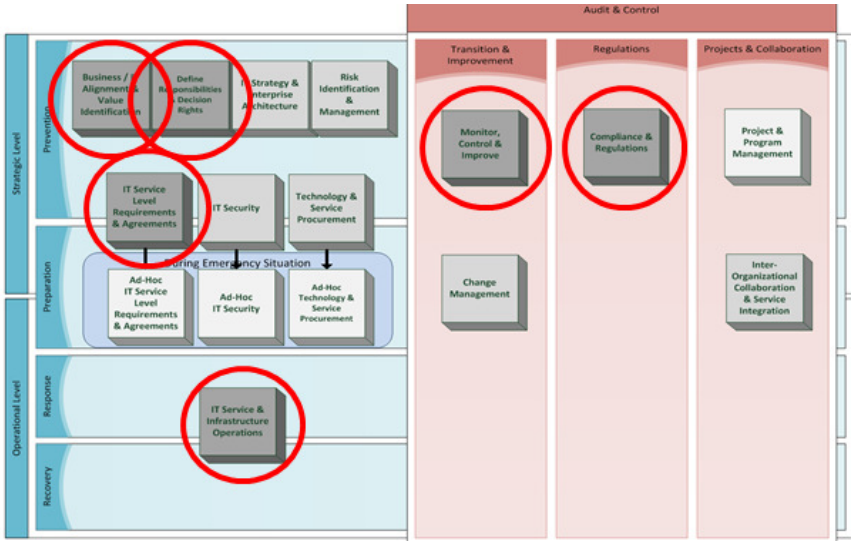


Figure 45: ITOCO4EM Core Process

Business / IT Alignment & Value Creation

This core process should support EM organizations to define and align IT initiatives and services to critical EM processes. Its sub-processes will help to:

- Implement an IT Governance culture
- Identify IT related requirements
- Estimate the value and benefits of IT initiatives for EM operations
- Generate a balanced and foresighted IT portfolio and by prioritizing the right IT initiatives

Define Responsibilities & Decision Rights

This core process should support EM organizations to define effective and efficient organizational structures to govern their IT. Its sub-processes will help to:

- Strengthen the cooperation between IT and EM operations
- Implement effective functions and committees to align EM and IT strategies and business/IT architectures
- Cope with changing organizational structures and IT Governance related decision rights

IT Service Level Requirements & Agreements

This core process should support EM organizations to define required IT services and service level agreements. Its sub-processes will help to:

- Define and use an IT service catalogue
- Determine service levels
- Ensure the quality of offered and used IT services

IT Service & Infrastructure Operations

This core process should support EM organizations to implement effective and efficient IT operations. Its sub-processes will help to:

- Define IT operation processes, which go in line with EM operations

- Implement effective IT functions, escalation methods and best practices
- Ensure the maintenance of IT systems and their functions

Monitor, Control, & Improve

This core process should support EM organizations to monitor and improve their IT services and related processes. Its sub-processes will help to:

- Define key performance indicators
- Measure, assess, and report IT operations performance
- Identify space for improvements and implement and follow a continual improvement process
- Reduce errors and malfunctions

Compliance & Regulations

This core process should support EM organizations to ensure the compliance of IT services, IT enabled processes and IT infrastructures. Its sub-processes will help to:

- Identify legal and regulatory requirements
- Evaluate and improve their degree of compliance

Optional Processes

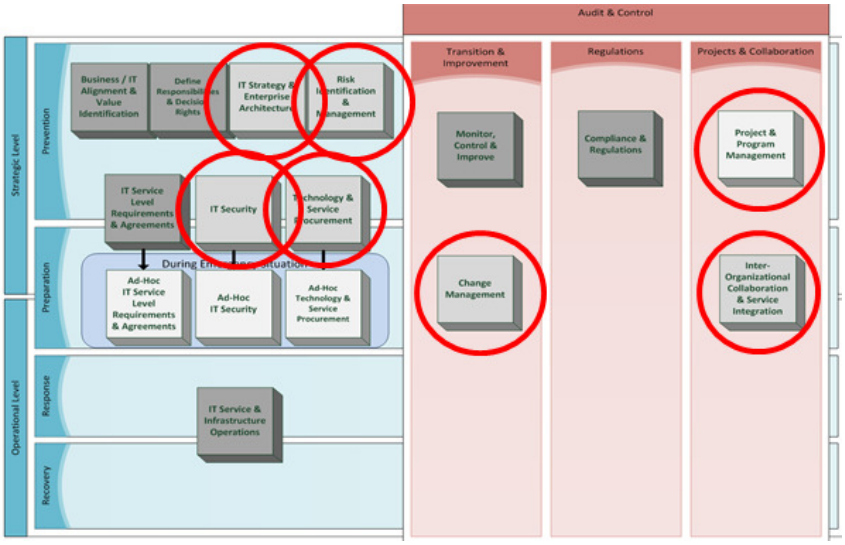


Figure 46: ITICO4EM Optional Processes

IT Strategy & Enterprise Architecture

This optional process can be implemented in a second stage. It should support EM organizations to define and align IT initiatives and services to critical EM processes. Its sub-processes will help to:

- Identify a suitable IT architecture
- Ensure that all IT and EM processes are considered in an IT strategy
- Consider current and future trends
- Implement and establish IT standards for increased compatibility and simplified maintenance

Risk Identification & Management

This optional process can be implemented in a second stage. It should support EM organizations to identify and manage risk associated with IT services and initiatives. Its sub-processes will help to:

- Identify crucial EM processes, which are enabled or supported by IT services or IT infrastructures
- Develop risk assessment and risk management procedures
- Manage risky suppliers, service providers and IT initiatives

IT Security

This optional process can be implemented in a second stage. It should support EM organizations to implement IT security processes. Its sub-processes will help to:

- Implement an IT security management
- Secure sensitive data and infrastructures
- Enable long-term communication and data exchange strategy with other organizations

Technology & Service Procurement

This optional process can be implemented in a second stage. It should support EM organizations to manage supply and procurement of IT assets and services. Its sub-processes will help to:

- Define a sourcing strategy
- Manage suppliers and service providers

Change Management

This optional process can be implemented in a second stage. It should support EM organizations to manage changes in the IT infrastructure and IT enabled processes. Its sub-processes will help to:

- Define an effective and efficient change process
- Ensure the quality of changes
- Provide a “trustworthy” and reliable IT infrastructure

Inter-Organizational Collaboration & Service Integration

This optional process can be implemented in a second stage. It should support EM organizations to foster inter-organizational collaboration. Its sub-processes will help to:

- Define inter-organizational standards
- Align their IT initiatives and enable co-sourcing
- Strengthen trust between EM organizations and simplify information exchange

Project & Programme Management

This optional process can be implemented in a second stage. It should support EM organizations to manage IT related projects and programmes. Its sub-processes will help to:

- Establish a project, programme, and portfolio approach to increase leverage effects between IT initiatives
- Implement project management standards

Ad-Hoc Processes

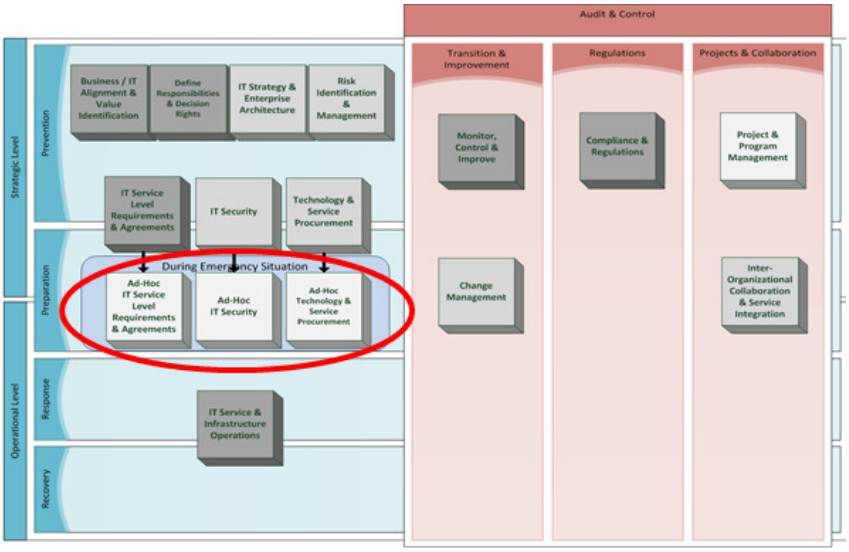


Figure 47: ITICO4EM Ad-Hoc Processes

These optional processes are derivatives from strategic processes. They rely much on their parent processes but need a closer look on their ad-hoc capabilities. In some cases, particularly if ad-hoc teams are involved, emergency situations demand a quick adaptation of processes. Hence, these ad-hoc processes focus on the requirements at the beginning or during an emergency. Its sub-processes will help to:

- Increase an EM organizations flexibility and ability to adapt to unforseen situations
- Keep a certain level of rigor to ensure the quality and security of IT services and data

9.1.3.3 ITICO4EM Implementation Scheme

ITICO4EM was designed to adapt to different EM organizations. During the research project it became clear that the most crucial distinction between the researched organizations is their size. Larger EM organizations have usually a higher IT Governance maturity, better IT related capabilities, and more resources. Smaller EM organizations are usually limited with regard to time and money. The following table shows an implementation scheme for small, medium, and large organizations.

EM Organization Type / Methods Areas	DR	B/ITS	ITTS	ISR	ITSA	ITS	ITP	AH Ser	AH Sec	AHP	SIOp	C&A	C&R	CM	CSI	IOPM	PM
EM Small	X	X	X	X	X	o	o	o	o	o	X	o	x	x	x	o	o
EM Medium	X	X	X	X	X	x	x	o	o	o	X	x	x	X	X	x	x
EM Large	X	X	X	X	X	X	X	x	x	x	X	X	X	X	X	X	X

Table 8: ITICO4EM Implementation Recommendation

The dark grey cells have to be implemented, medium grey cells should be implemented, and white cells can be implemented.

This implementation scheme is not put in concrete, it should rather be seen as a guideline for EM organizations. The actual demand has to be identified individually.

9.2 IT-ORG / CrIO: Organizational Improvements in EM

The top managers in industry realize that the governance of IT can have a significant impact on the success of the business. Therefore, the issue of IT-Business alignment is under the Top 3 IT Management concerns from 2003 to 2010 (Luftman & Ben-Zvi, 2010).

However, strategic IT alignment cannot be achieved by technological and methodological considerations only. Moreover, Weil and Ross (2004, p. 158) state, “effective IT Governance requires harmonization of all …components” of a framework, but “enterprise strategy and organization sets the direction”. Amongst other factors the IT Governance Institute (2003, p. 6) describes two organizational aspects as crucial for the success of IT Governance, which consequently should help the organizations to achieve strategic alignment of IT initiatives and create value from them:

- “Providing organisational structures that facilitate the implementation of strategy and goals
- Creating constructive relationships and effective communications between the business and IT, and with external partners”

Both aspects have been identified as not optimal in the researched EM organizations. This was mainly due to the shifting responsibilities during escalations and the “ad-hoc teams”, but also because IT is not seen as an enabler and therefore not in the responsibility of key decision-makers. Hence,

the given structures are sub-optimal for good IT Governance. Section 7.2.2 has elaborated on these organizational issues in more detail.

The connection between strategic IT alignment, strategic objectives, and stakeholder values is described in the following figure:

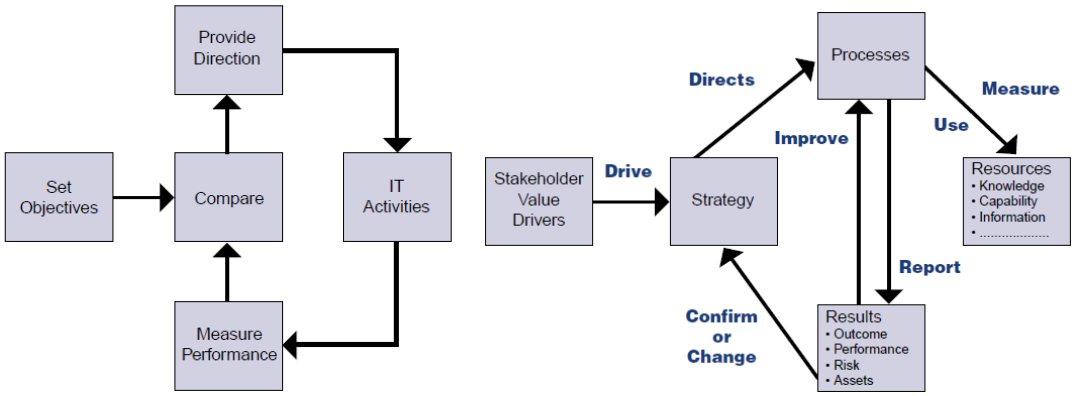


Figure 48: Strategic Objectives & IT Activities / Stakeholders and IT Governance Process (IT Governance Institute, 2003, pp. 12, 21)

The strategic objectives (outer left of the left model) are defined by the stakeholders (outer left of the right model), these objectives provide a direction (top of left model), which drive the IT strategy and direct IT enabled processes (top of right model). Consequently, aligned IT activities are utilized in IT enabled processes (outer right in left and right model), which need to be constantly measured and assessed in order to improve an organizations performance (bottom of left and right model). These two models make clear how important the involvement of stakeholders in an IT Governance process is, without the right stakeholders the strategic objectives and consequently the IT strategy would be not in line with each other which would result in a misleading direction of for future IT initiatives and misguided performance indicators. Subsequently, IT cannot be aligned even if all other circumstances are given.

Therefore, the organizational structure has to be geared up for this purpose and responsibilities, accountabilities, roles, functions, and committees have to be defined and integrated into the organization. Also clear decision processes have to be defined to support an IT initiative's life cycle. The strategic alignment of an investment portfolio is not enough on its own, to create value from the chosen IT initiatives they have to be monitored until their retirement (E.g., a good IT services is worthless if the service quality is too low).

However, such structures have to be a bit different in EM organizations due to the changing responsibilities, inter-organizational collaboration, and lack of resources. Weill and Ross (2004, pp. 14, 17) state that “effective IT Governance requires a significant amount of time and attention” from top management and needs to be “carefully designed and implemented” to support the IT decision making process. They also state that good IT Governance “facilitates learning by formalizing exception processes. Enterprises often learn through exceptions – where a different approach from standard practice is used for good reasons”. This is even more the case for EM organizations, which have to deal with temporary structures and uncertain situations. It is therefore necessary to use IT Governance structures, which can cope with such issues and enable EM organizations “to adopt new processes that apply new technologies effectively”.

From the IT decision rights matrix shown in Chapter 7.2.2 (Table 5, p.159) it became clear that these IT decision rights are often not optimal and that the IT and EM operations need to make more conjoint solutions. It also became clear that smaller EM organizations do not have the skills and resources to take a leading role in IT Governance, and that some decisions need to be made across an organization’s boundary in order to be effective. The following sections will therefore elaborate on the proposed organizational structures, roles, and committees for EM organizations.

9.2.1 The most appropriate Archetypes to Govern IT in EM

To design an IT Governance structure for an organization it is important to know the underlying strategic principles. One way to distinguish an organization’s strategic principles is the concept of “value disciplines”, which can be split into three categories (Treacy & Wiserna, 1996; Weill & Ross, 2004):

- **Operational Excellence:** The focus lies on efficiency and reliability, cost reduction, and improvement of internal processes, and streamlining of the supply chain.

- **Customer Intimacy:** Aims toward the long-term value of the company, by cultivating customer relationships and individual solutions.
- **Product Leadership:** The main driver is the rapid commercialization of new and innovative products and implementation of new ideas.

From these descriptions, it is clear that not only their strategic goals will differ but also how they govern their IT.

EM organizations have usually not-for-profit character and do not aim for long-term customer relationships. Hence, the researcher excluded “Customer Intimacy” and “Product Leadership”, and focused on “Operational Excellence”. This assumption can also be confirmed by impressions during the case studies where the researched organizations generally focused on the streamlining of processes and the increase of efficiency and reliability. However, it became also evident that due to the interwoven structure of public administration, EM units, IT departments, and CIPs, IT decisions have a far-reaching effect, yet IT decisions are not made conjointly. Therefore, the researcher proposes the following IT Governance structure as shown in Figure 49.

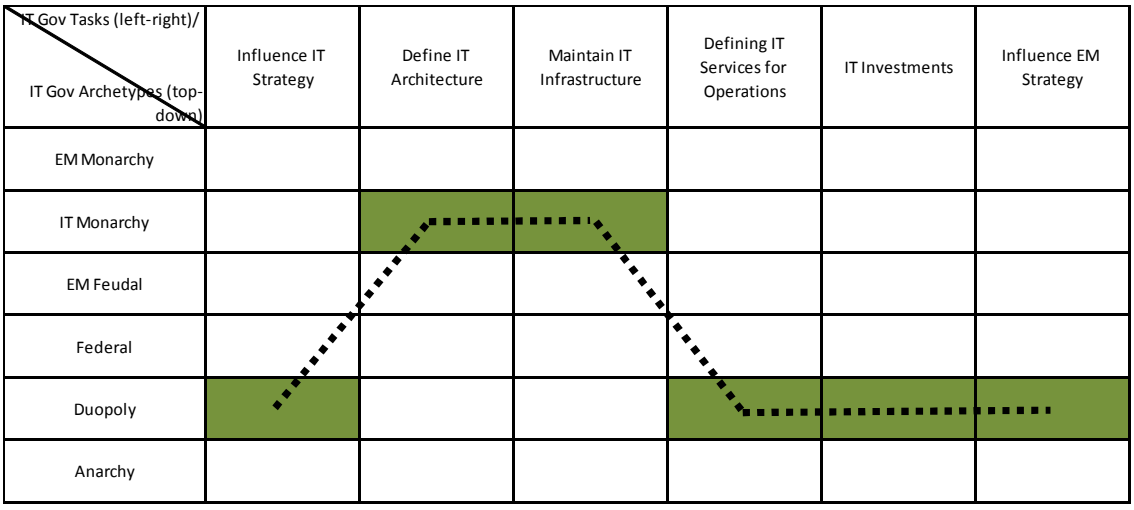


Figure 49: Proposed IT Governance Arrangement Matrix for EM Organizations

As one can see the main IT Governance archetype is “Duopoly”, only the very specific IT disciplines are the sole responsibility of the IT department. Duopolies enable EM organizations to pursue the two underlying assumptions. First, they can help to streamline processes since experts from both fields can use their knowledge to shape them accordingly. Second, duopolies have the character of committees, which can easily expanded to enable the communication between

departments and across organizations that in turn can improve the whole EM process. Moreover, this becomes increasingly important when we look at Figure 48. The significance of the involvement of the right stakeholders is eminent in order to form a suitable IT strategy. The Duopoly enables them to make conjoint decisions and find the right balance of aligning IT initiatives and IT services with EM requirements and shaping EM strategies with the technically possible. Certainly, this will limit an EM unit's flexibility to implement individual solutions, but it will also increase the overall performance of EM operations and will make the implementation of future IT initiatives easier due to a shared IT vision and IT architecture. The positive effects of such a structure can be seen in Major Case 1 (MAC1).

9.2.2 Internal and Inter-Organizational Committees

Since, the leading IT Governance archetype is a duopoly, the use of committees to make conjoint decisions is highly recommended. Even though not-for-profits and public administrations make use of committees extensively, only one researched organization (MAC1) has used committees to steer IT initiatives for EM purposes. However, this organization outperforms the other researched organizations in terms of IT utilization, streamlined processes, and even cross-organizational IT integration. Additionally, their IT Governance maturity was relatively high. During the interviews it became also clear that both, IT staff and EM operations, value the committees and see them as an effective way to come to conjoint solutions. Consequently, IT enabled processes are accepted and IT infrastructures support cross-organizational information exchange. These parameters indicate that IT committees should also be used by other EM organizations. Therefore, it is proposed to implement two committees to govern IT within and across EM organizations:

- **Internal IT Governance Committee**: The internal IT Governance steering committee will help to align internal processes and IT initiatives. It should consist of at least one representative of the IT Unit, Emergency Operations, Emergency Management, and Finance. If the EM Unit is a subordinate department of a larger public administration the committee

should be expanded by an IT representative and a general manager of the public administration.

- **External IT Governance Committee**: Since most emergency situations demand the cooperation of multiple organizations and administrations, it is proposed to implement a cross-agency IT Governance steering committee. Such a committee can assure that IT initiatives, which affect external communication and EM processes, are aligned across EM organizations and administrations. Consequently, it will increase the interoperability of IT systems and enable EM operations to improve their information flow. It will also help to implement standardized technologies across organizations. Moreover, it will generate a platform to exchange experiences between the participating organizations, which can help smaller EM organizations to "do the right thing" without having to go through a "trial and error" phase.

Even though, committees can be a good instrument to steer IT initiatives and come to conjoint decisions, it must be assured that such committees have the power to make quick decisions. Implementing myriads of committees can slow down the decision process and then become counterproductive. Even worse, if committees are deliberately circumvented to avoid lengthy decision processes "IT grey zones" can arise, which are neither documented, nor do they fit into the overall IT strategy or infrastructure. Therefore, it is important to keep the administrative work at a minimum and elect reliable and goal-oriented committee members.

9.2.3 A new Role: The Crisis Information Officer (CrIO)

In some cases, it might not be feasible to implement a full blown IT Governance steering committee, which can be the case in small and medium EM organizations. However, it is still necessary to make conjoint IT decisions between EM and IT and define a shared IT strategy.

Moreover, even large EM organizations with an IT Governance committee structure might need a central function, which can translate and mediate between the EM operations and IT unit, or oversees the current and planned IT initiatives.

Hence, it is proposed to introduce the role of a “Crisis Information Officer” (CrIO). The CrIO, is the EM counterpart to a classic Chief Information Officer (CIO). A CrIO should be responsible to document and examine ongoing and planned IT / EM driven initiatives in order to identify potential improvements. Therefore, it is necessary that the CrIO has a strong expertise in EM procedures and a good background in IT.

By having both EM and IT knowledge CrIO can take over the function of an “ambassador” between IT and EM. Understanding the needs of the EM operations and being able to assess the capabilities of current technologies a CrIO would be an ideal role to align IT with EM needs, but also influence the EM strategy by IT’s capabilities.

9.3 IVEM²: A Modular IT Value Estimation Method for EM Organizations

As described in Chapter 7.2.1 the EM/IT alignment process will be an almost impossible task for multiple scenarios since some goals and processes might compete. For example, it could be the case that IT investments are “optimized” for a particular scenario, but these investments are of lesser value in other emergency situations. Moreover, an alignment method based on rigid and predefined emergency situations is not suitable for yet unknown threats since it is too inflexible. Changing such strictly planned emergency situations to address an upcoming and unknown situation will take too much time and effort. It can also negatively influence an Emergency Management team’s effectiveness and efficiency since the actual situation is very different from what was rehearsed in emergency drills. Consequently, strictly coupled IT services might also not work as expected. Therefore, this thesis proposes a conceptual IT value estimation method, which enables EM organizations to align their IT initiatives with reusable modules (also described as “recurring patterns” or “set of actions” (e.g. evacuation, search for missing people, etc.) in chapter 7.2.3.

9.3.1 Analytical Hierarchy Process (AHP)

The proposed IT Value Estimation Method for EM (IVEM²) uses the Analytical Hierarchy Process (AHP), which will be explained briefly as an introduction to

the IVEM² method discussed in chapter 9.3.2. AHP was developed by mathematician Thomas L. Saaty in the 1980's. It is a decision support method for to simplify complex decisions and make rational decisions and will therefore be explained briefly (Saaty, 1987, 1990).

The goal of the AHP is:

- Support decisions in teams
- Find joint solutions within a minimum of time
- Increase the transparency of the decision-making process and make results comprehensible to everybody
- Uncover inconsistencies in the decision-making process

AHP provides:

- Review and enhance subjective "gut decisions"
- qualitative weighting based on comparative decisions
- structured and hierarchical representation of a final decision by a decision tree

The AHP-Method is "hierarchical", because the criteria, which is used to solve a problem, is in a hierarchical order. Elements of a hierarchy can be divided into groups, to refine and simplify the decision-making process. It is "analytical" because it describes and analyses the constellation and dependencies of the particular problem, and it is a "process" because it follows a defined and repeatable procedure.

9.3.1.1 Phases of AHP

According to Saaty (1987, 1990) the decision process is divided into three phases. In the following section, the methodology of the AHP approach will be shown.

Phase 1: Collecting the data

At this stage of the decision-making process all data has to be collected that is relevant for an accurate decision. Thus, this part requires thorough attention because the rest of the process will be based on the results of this phase.

The first step is the exact formulation of the question that has to be answered by the decision-making process. The aim of the question is to find the best solution or answer to the problem. In this case the general question is: “Which IT initiative delivers the highest value for EM operations”.

In the second step of the process, all relevant criteria to solve the issue have to be collected, this can be done by a brainstorming process such as mind-mapping. The collected criteria can be in an unsorted order, as for now it is just important to gather all the important aspects. In this case, the strategic priorities of the EM organizations were an excellent resource, but in general, it can also be developed from scratch or by the means of an already existing collection.

In the third step, all alternatives collected during step two have to be reviewed and summarized to a question catalogue, which should be as detailed as necessary but as simple as possible. This is a rather tricky decision, because the more criteria we use the more complex the questionnaire will become, but not necessarily more accurate in its results. Thus, this is one of the most important steps in this method. Even though errors can be made in this stage, they can be corrected over the time easily. Due to the hierarchical structure of the AHP method, criteria can be changed or reweighted whereas only the changed groups must be reviewed rather than the whole question catalogue.

Phase 2: Compare and weight data

In this phase, the weighting of each criterion will be determined. Thus, the fourth step is a pairwise comparison of each criterion. By this method, a decision maker can get a very precise assessment from the multitude of competing criteria. This leads to a ranking for each criterion according to their importance. To simplify this step, related criteria should be grouped as suggested in step three, thus only related criteria and groups have to be compared pair-wise. Consequently, the whole hierarchical structure becomes clearer and more structured. For the evaluation a Likert-scale (Likert, 1932) with a bandwidth from 1 to 9 points is used.

Phase 3: Data processing

The fifth and last step is to balance out inconsistencies of step four. Inconsistencies can occur when at least three criteria are rated against each

other, hence it can happen that the criteria is rated as following: A > B, B > C but C > A. Therefore the pairwise comparison C > A would be inconsistent. Thus, AHP uses a mathematical model to get a more precise weighting of all these criteria, which is done by the so-called "Eigenvector" and “Eigenvalues”. By an iterative use of this mathematical method, the decision matrix will be normalized and therefore the ranking becomes more coherent and criteria will less likely contradict to each other, which will increase the overall accuracy and stability of the solution.

9.3.1.2 Advantages & Disadvantages

A clear advantage of AHP is that it is able to handle all kind of complex issues, such as strategic decisions. Additionally it provides the flexibility to simplify their complexity but at the cost of accuracy. Compared to other decision making methods such as decision tables and weighted scoring, AHP provides a more accurate and transparent solution that is repeatable and comprehensible. This is particularly important for group decisions or decisions that are made in a company so every party can reproduce the result and check its reasonability. Due to the increased transparency and the breakdown structure to pairwise comparison of relevant criteria, subjective decisions about the weighting are minimized. The subjectivity can be even more reduced if the pairwise comparisons are conducted independently by different experts. The different results can then be summarized to an average for each criteria, which will result in a normalized rating for each criterion and single deviations will be mitigated. However, there are still critics who say that the AHP method is still too arbitrary to make 100% objective decisions. It can also be very time consuming to develop and conduct the questionnaires, which reduces the acceptance of such an approach (Saaty, 1987, 1990). Nevertheless, the AHP method was chosen over simpler decision-making methods because it is more accurate and flexible in many ways.

9.3.2 IT Value Estimation Method for EM (IVEM²) based on AHP

Instead of using rigid plans for emergency situations as a basis for an alignment method, the researcher developed a modular approach to tackle the

"IT value estimation" issues identified in Figure 29 (p.152). The researcher followed this modular idea since the process analyses in the case studies (see Appendix D (Model & Process Documentation)) have shown that most emergency situations have recurring patterns (set of subroutines or activities such as evacuation, search for missing people, supply water, supply shelter etc.), which can even be used in unknown scenarios. Therefore, decomposing rather complex emergency situations in smaller but reusable chunks (referred as modules in IVEM²) enables an Emergency Manager to evaluate their impact in several emergency situations, which helps the EM organization to identify the most crucial activities. In turn, it is easier to evaluate the impact of an IT initiative (e.g. exchange of hardware, software update, new IT-project) against modules rather than a number of complex and highly volatile emergency situations. Such a decomposing technique is also used in other domains where flexibility and reusability are highly demanded (T. Chan, Fielt, Gable, & Stark, 2010; R. B. Chase, Jacobs, & Aquilano, 2006; Hedin, Ohlsson, & McKenna, 1998).

Moreover, the researcher was able to identify that crucial modules (e.g. evacuation) are more likely to be used in emergency situations than less important modules. Therefore, it was concluded that an improved alignment of IT initiatives with these "high impact" modules will most likely increase EM operation's performance in all affected emergency situations, in which these modules are used. Since the utilization of these "high impact" modules is higher than of other modules, there is an increased likelihood that "high impact" modules will also be used in yet unknown scenarios, a phenomenon that could be explained with the "Conjoint-Analysis" (Tsafarakis, Delias, & Matsatsinis, 2010; Tsubouchi & Takata, 2007).

The modular "IT Value Estimation Method for Emergency Management (IVEM²)" as shown in Figure 50 enables an EM organization to build a hypothetical IT portfolio and prioritize initiatives according to their benefits and risks in order to gain maximum process value from EM critical IT services.

The granular breakdown structure enables EM organizations to handle smaller and more manageable packages, which make it easier for IT and EM personnel

to anticipate the benefits and risks of used technologies. As a result, this would increase trust in and value realization of IT investments.

The researcher applied an adapted and enhanced version of the “Community Value Estimation Method” (CVE), which is based on the Analytical Hierarchy Process (AHP) and has been successfully tested in a large municipality to align IT projects with community values (Vogt & Hales, 2010). The underpinning steps of IVEM² are described in the following sections.

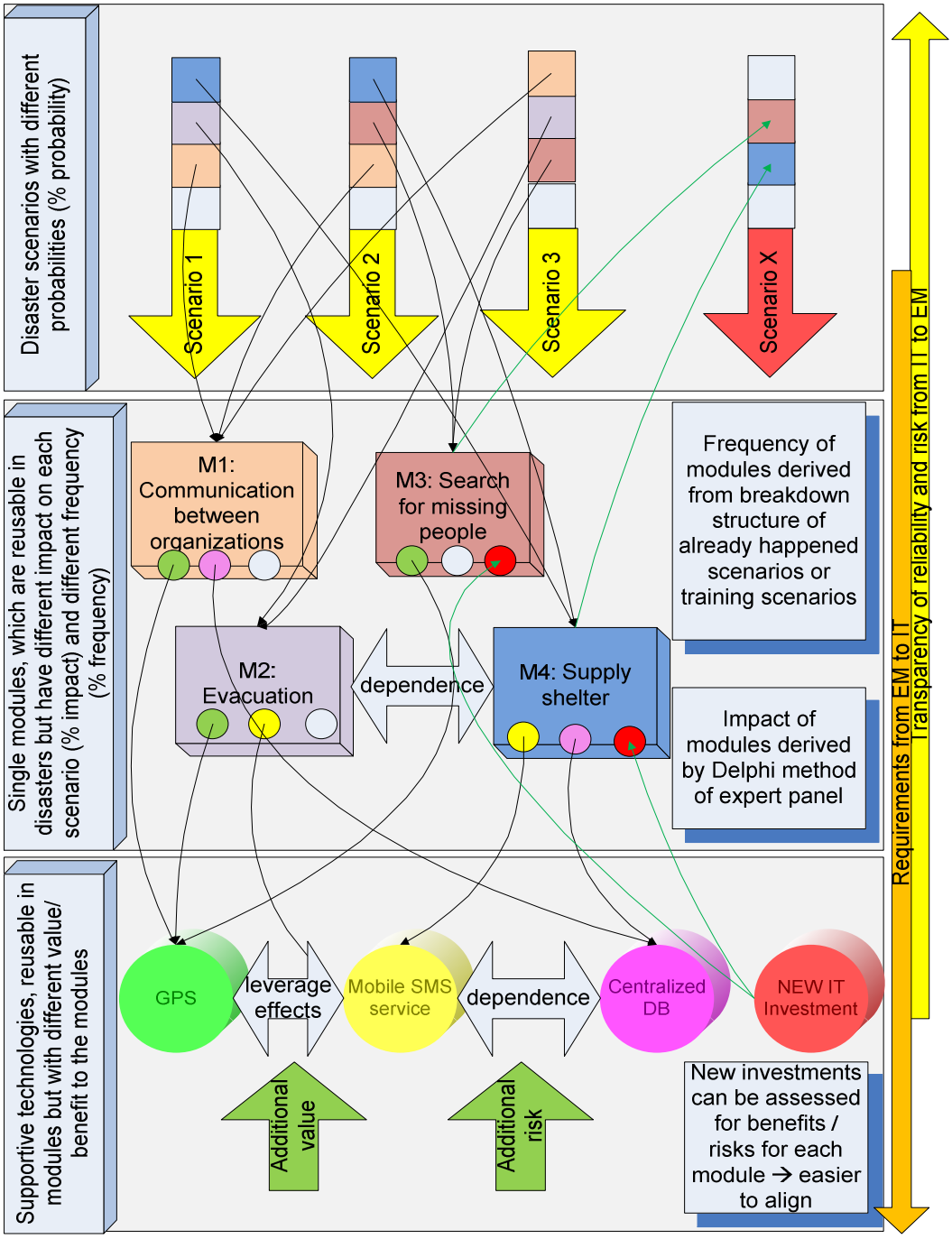


Figure 50: Modular approach

The following influence factors are relevant for this method; simple examples are used to explain the process:

1. Probability and impact of a particular scenario (PI), derived by AHP pairwise comparisons (or alternatively by statistics)
2. Impact factor of a module/pattern for a known or possible scenario, derived by pairwise comparison (MI)
3. Impact factor of an IT service for each module, derived by pairwise comparison (SI)
4. Impact factor of a technology for each IT service, derived by pairwise comparison (TI)

TI = Total Technology Impact

T = Technology Impact per Service

SI = Total Service Impact

S = Service Impact per Module

MI = Total Module Impact

M = Module Impact per Scenario

PI = Probability & Impact of a Scenario

m = Number of possible scenarios

n = Number of identified modules

p= Number of IT Services

q = Number of Technologies

$$TI_i, SI_j, MI_k PI_l \in [0,1] \forall i, j, k, l$$

$$\sum_{i=1}^{q} TI_i = 1$$

$$TI_i = \sum_{j=1}^{p} T_{i,j} * SI_j$$

$$SI_j = \sum_{k=1}^{n} S_{j,k} * MI_k$$

$$MI_k = \sum_{l=1}^{m} M_{k,l} * PI_l$$

Therefore:

$$TI_i = \sum_{j=1}^{p} T_{i,j} * \left(\sum_{k=1}^{n} S_{j,k} \left(* \sum_{l=1}^{m} M_{k,l} * PI_l \right) \right)$$

Figure 51 will give an example of how IVEM² and the AHP technique are applied in a simplified example. Due to the space restrictions and readability, the figure shows only three alternatives for each hierarchy. Therefore, it must be said that IVEM² and AHP are not bound to these restrictions. The systems is independent of the numbers of hierarchies and independent about the number of alternatives for each hierarchy. This is also represented in the formula where each hierarchy uses a different letter for the Sigma index. However, it should be

noted that AHP demands the user to compare each alternative even though it might not be used (e.g. Module 2 might not be used in Scenario 3). In such a case the alternative performs very bad compared to other alternatives. Even though the impact is not 0 in this case, it will not influence the final result significantly and can be neglected.

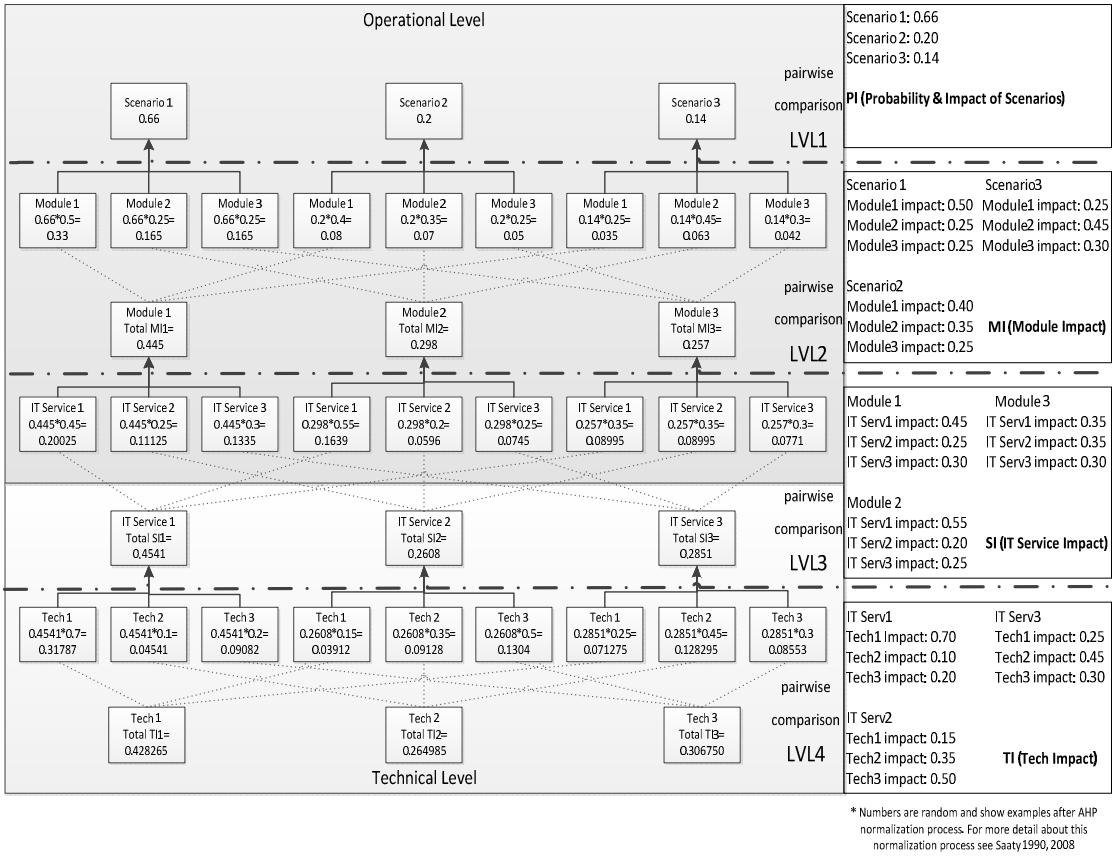


Figure 51: AHP Process

The “Total Impact” of an IT technology can therefore be calculated, and a technology investment to improve the desired IT services would be prioritized as follows:

1. **TECH 1**, with an impact factor of 0.428265
2. **TECH 3**, with an impact factor of 0.306750
3. **TECH 2**, with an impact factor of 0.264985

Example TI for TECH1:

$$TI_i = \sum_{j=1}^{p} T_{i,j} * SI_j$$

$$TI_1 = \sum_{j=1}^{3} T_{1,j} * SI_j = T_{1,1} * SI_1 + T_{1,2} * SI_2 + T_{1,3} * SI_3$$

$$TI_1 = 0.7 * 0.4541 + 0.15 * 0.2608 + 0.25 * 0.2851 = 0.428265$$

To calculate the numbers shown on the right side of Figure 51, the researcher utilised Likert-scales (Likert, 1932) for each pair-wise comparison, these are scaled from 1 to 9 either side, whereas 1 marks the neutral point which means that both goals are equally important and 9 marks that this goal is extremely more important than its opposite. E.g. if "Module 1" should be favoured very strongly (7) over "Module 1" it must be marked as follows:

"Module 1" 9 - 8 - (7) - 6 - 5 - 4 - 3 - 2 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 – 9 Module 2"

If "Module 2" should be favoured moderately (3) over "Module 1" it must be marked as follows:

"Module 1" 9 - 8 - 7 - 6 - 5 - 4 - 3 - 2 - 1 - 2 - (3) - 4 - 5 - 6 - 7 - 8 – 9 "Module 2"

The following scale (Table 9) was used to determine the importance of each pair:

The Fundamental Scale for Pairwise Comparisons		
Intensity of Importance	**Definition**	**Explanation**
1	Equal importance	Two elements contribute equally to the objective
3	Moderate importance	Experience and judgment slightly favor one element over another
5	Strong importance	Experience and judgment strongly favor one element over another
7	Very strong importance	One element is favored very strongly over another; its dominance is demonstrated in practice
9	Extreme importance	The evidence favoring one element over another is of the highest possible order of affirmation
Intensities of 2, 4, 6, and 8 can be used to express intermediate values.		

Table 9: Pairwise comparison scale according to Saaty (1990)

The total technological impact factor (Total TI) will allow us to rank IT services and / or technologies according to their value to the EM process. To build an optimized portfolio EM Organizations will have three options:

1. *"Total TI Threshold"*: This is only interesting for EM organizations that have either no budget constraints. They can define a threshold and invest only in those projects which have a minimum TI factor (e.g. they will pursue all project with an TI >= 0.3, regardless of what the cost are)
2. *"Cost/Benefit"*: This is mainly interesting for EM organizations, which have to justify their investments. However, this will force them to know the costs for each proposed investment (ITCost) (e.g. projects with TI >= 0.1 will only be pursued if investment is <=$20,000, projects with TI >= 0.3 will only be pursued if investment is <=$100,000, …)
3. "*Maximum Budget*": This will be most interesting for those organizations that have a fixed budget. However, two more variables must be known: First, the cost for each proposed investment (ITCost) and second their maximum budget for IT investments (MaxBudget). In the second step the portfolio can then be optimized according to these constraints.

It can therefore happen in option 2 & 3 that projects of lesser TI will be given priority over projects with higher TI since their cost/benefit factor is higher.

Besides clarifying "gut decisions", a major advantage of this AHP based method is that every EM organization can adjust the level of complexity towards their capabilities and needs. Large EM organizations with many IT projects and a more complex process structures can add extra hierarchies if needed and divide the decision process in "technical" and "operational" level. Consequently, the method will become more accurate because decisions are made by experts in the field and the increased granularity is more precise. However, the initial setup of the method will become increasingly complex the more hierarchies are added. Smaller EM organization can simplify the hierarchical structure and pairwise comparison and use only those elements, which they feel are appropriate (e.g. merge IT Services and IT Technology hierarchy in Figure 51 since in smaller organizations IT services are often associated with particular technologies [e-mail → e-mail server]). Since these smaller EM organizations

have usually less technological projects in line and processes are not that complex this should be a reasonable action that would not alter the results too much.

In larger EM organizations, it might not be enough to calculate the technological impact factor in order to prioritize investments and spend money and resources for them. As Figure 52 in Chapter 9.3.3 shows there might be dependencies, leverage effect, and risks associated with some technologies or services. Therefore, the following two sections will discuss possible “add-ons” for the proposed IVEM² method. Following the modular approach, these are not mandatory but they definitely have positive side effects and should be considered.

9.3.3 Interdependencies and Leverages

Information is the primary source to manage a crisis and mitigate its effects. The harder a disaster strikes the larger the crisis. The bigger the crisis is the more information is needed to coordinate participating EM organizations and resources. With an increased information demand we need sophisticated information systems, IT services, and technologies to cope with it. The more IT services and technologies are used or proposed in an organization the more they are usually connected. Hence, we can gain leverage effects if an organization invests in new technologies and services that is supporting existing assets in the same hierarchy. E.g. if an EM organizations would invest in a new alarm system without considering to invest in an appropriate network the investment might be not be as valuable as expected since the supporting network service might not be reliable enough. Therefore, technologies and services should be aligned as a whole system.

The modular IVEM² approach is particularly suited for this purpose. As soon as all elements (scenarios, modules, IT Services and supporting technologies) are known and recorded one can model dependencies between technologies by attaching weighted variables to each service and /or technologies. Figure 52 shows a visualized example of a simple constellation.

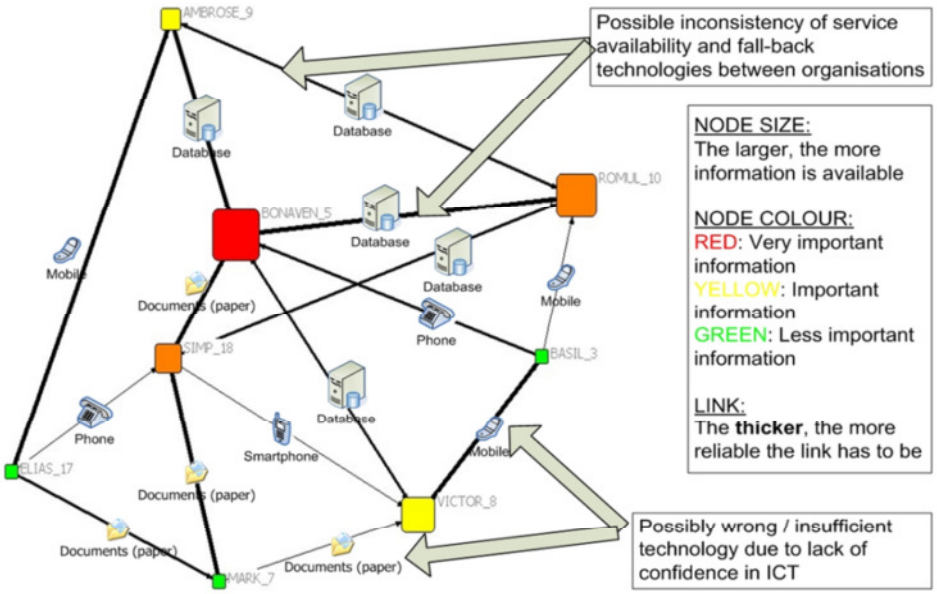


Figure 52: Dependencies and leverages

By combining the results of the AHP based value estimation methods with the peer-to-peer dependency variables of each technology EM organizations should be able to identify “investment clusters” as shown in an example below (Figure 53).

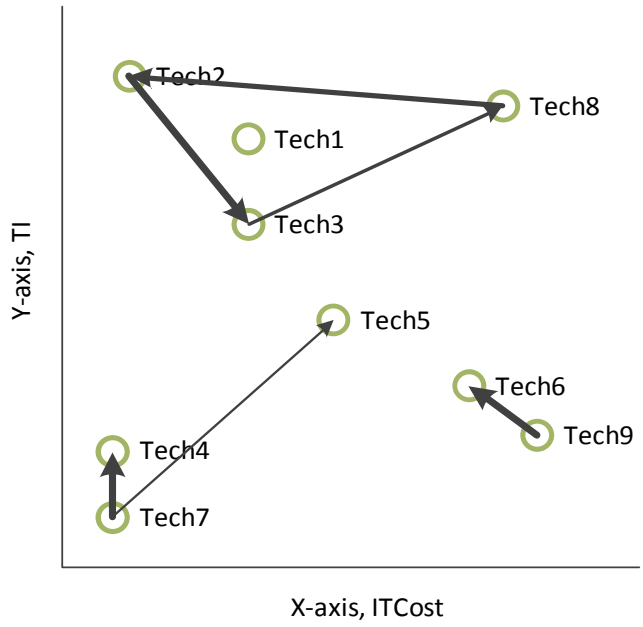


Figure 53: leverage effect clusters

The initial prioritization is based on technological impact (TI, y-axis) and costs associated with the IT projects (ITcosts, x-axis) as described in the previous

section. Dependencies are shown as connections between the technologies. The thicker a connection, the more the technologies are associated to each other, the higher is the leverage effect and interdependency.

Figure 53 shows two small clusters and one large cluster, which should be considered if a technology has to be chosen. E.g., Tech4 has a higher TI but the same costs as Tech7, without the leverage cluster information the choice would be in favour of Tech4. However, using the leverage clusters reveals that Tech7 has positive effects on Tech4 and Tech5, thus, these investments should be reconsidered. There should be similar considerations regarding the large cluster (Tech2, Tech3, and Tech8). Tech 8 might not be considered if we judge by a cost-benefit ratio only. However, Tech8 has a huge effect on Tech2, which is rather cheap, if the impact of Tech8 on Tech2 would increase TI of Tech2 significantly the overall cost-benefit ratio might be better than investing in Tech2 only.

The breakdown into modules enables EM organizations to handle smaller and more manageable packages, which makes it easier for IT and EM personnel to anticipate the benefits and risks of used technologies. As a result, this would increase trust in and value realization of IT investments. These processes are visualized in Figure 50 (p.205).

An additional advantage of this method is that IT services can be mapped to each module. In return, this will enable EM personnel to test scenarios in which important IT infrastructures fail, or track and manage mission critical IT services during EM situations to ensure that these IT services are managed proactively and deliver a high quality of service. The following section will describe this in more detail.

9.3.4 Increasing IT Service Quality During a Disaster and Prepare for the Uncertain

Besides prioritization of IT investments one of the major advantages of this modular approach is an increased transparency of essential modules, important IT services, and supporting technologies. Whenever a disaster strikes the flexibility of this method will allow EM organization to adapt to the situation.

As Figure 50 (p.205) shows, the down and upstream of IVEM² enables Emergency Managers to see which IT services and technologies are needed in order to support their attempts to manage a crisis. Therefore, their IT support staff can proactively manage the particular services and even increase availability and resources on demand if possible. They are also able to develop backup processes in case one or more of the services or technologies fail during a disaster. This will significantly increase trust in IT enabled process since accelerated processing times can be used, but the whole process will not fail in case of a system outage. The increased transparency will ensure that important systems are supported, maintained, and improved accordingly.

Another side effect is that EM organizations can easily adapt to unknown scenarios. Since Modules (such as “evacuation”) are frequently reused in known scenarios, possibilities are high that already existing modules can be reused in an unknown emergency situation. Therefore, the modular approach enables EM organization to “align to the unknown”. Whenever an IT service or technology supports an important module, the benefits can also be realized in a new scenario where this module is reused.

9.4 Discussing the IT/EM-Governance Approaches

As mentioned in the literature strategic IT alignment cannot be achieved by applying one single approach. In order to align IT with strategic objectives in an organization, different views, methods, and structures have to be used (IT Governance Institute, 2003; Van Grembergen & De Haes, 2009; Van Grembergen, et al., 2003; Weill & Ross, 2004). Hence, this research project tried to tackle the problem from different perspectives as shown in the following figure.

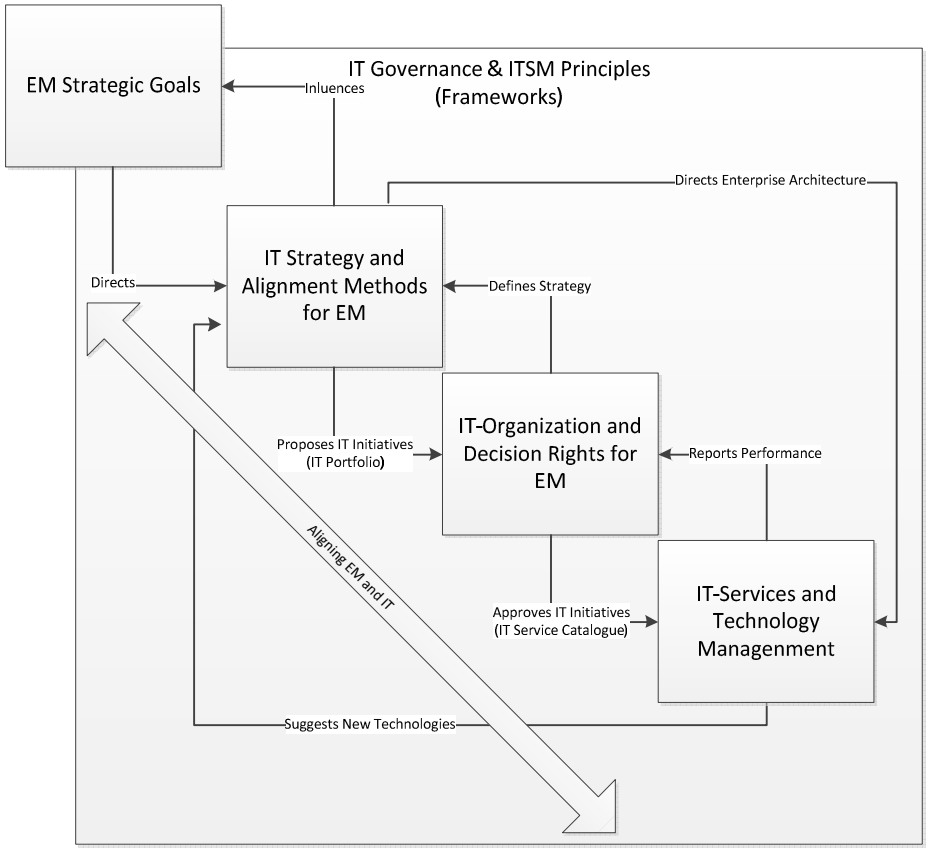


Figure 54: Combining Different Views on IT Governance in EM

To align IT initiatives with Emergency Management objectives the researcher had to tackle the three main issues of EM with IT Governance, which have been identified in Chapter 7.2. These are:

- Issues with existing IT Governance frameworks
- Organizational issues
- IT value estimation issues

Hence, the following three approaches have been combined:

ITICO4EM is a simplification and adaptation of COBIT and ITIL. It reduces the complexity of existing IT Governance frameworks only used processes, which are relevant for EM organizations.

IT-ORG/CrIO proposes the implementation of a “duopoly” structure for IT decisions, to ensure that EM and IT views guide the IT strategy. It also proposes the use of internal and external IT Governance steering committees and the implementation of a Crisis Information Officer (CrIO) in order to translate and mediate between EM and IT.

IVEM² addresses the last issue and should help EM organizations to estimate the value of IT initiatives towards their EM operations and build an optimized IT portfolio accordingly. This will align their IT initiatives with EM operations even in uncertain environments by using a modular approach based on AHP.

The tree elements together build the conceptual ITEM-Governance reference model. The following figure is illustrating this combination:

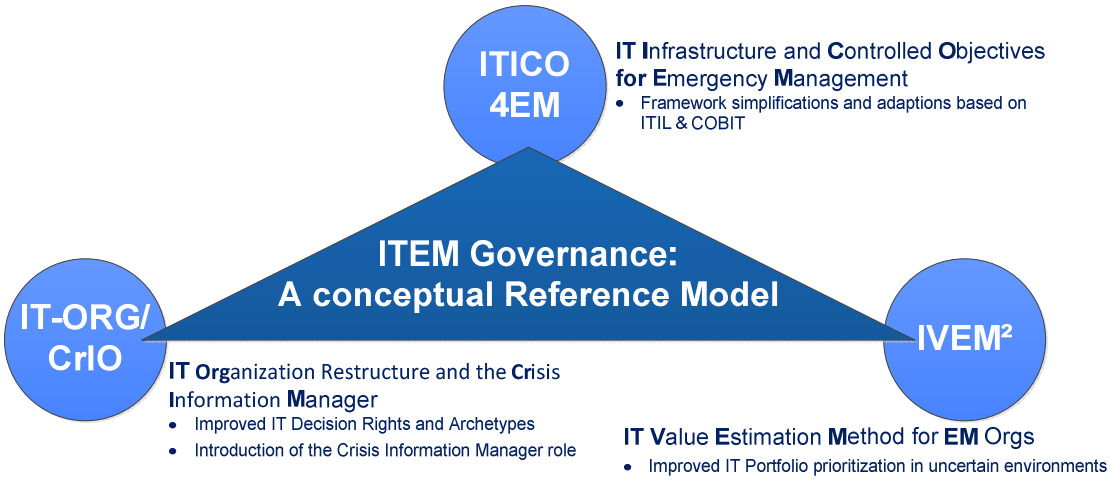


Figure 55: ITEM-Governance Approach

10 Evaluating the Conceptual Models & Methods

As Jayaratna (1994, p. 108) and Recker (2005, p. 5) describe it: “No problem-solving process can be considered complete until evaluation has been carried out. It is the evaluation which helps us to measure the effectiveness of the problem-solving process”. However, specific approaches for the explicit evaluation of conceptual reference models are not very common (Fettke, Loos, & Zwicker, 2005; Frank, 2007).

According to Frank (2000, 2007) conceptual models and methods are an important part of IS research since they largely influence the quality and development of information systems. Even though conceptual models in computer sciences are usually used to develop software requirements, they have been used in this research project to define the requirements of the EM domain with regard to IT Governance and IT Service Management processes. Although this approach is slightly different, the same rules for evaluation were applied.

However, the evaluation of such models and methods is challenging because they are usually based on different views (e.g. domain expert and programmer) and their input varies in granularity and quality. Such a variety of information sources and quality makes it almost impossible to use formalized specification language, which is accepted and understood by all participants. On the other hand, natural language is too complex and imprecise to describe certain processes and make them comparable. Hence, conceptual models and methods are used to fill this gap and give the researchers and participants a basis for discussion and further refinement, which should ultimately lead to more precise and formalized versions. Consequently, conceptual models and methods can utilize multiple design and modelling techniques, which enables the involved parties to communicate effectively. Moreover, conceptual models and methods are not focused to reflect reality in detail, but rather to find new organizational structures and process flows, in order to identify space for improvement and become reference models. Thus, a conceptual reference model does not have to reflect reality entirely, but it should also not oppose evidence. However, this diversity makes it hard to assess the results by sheer

quantitative approaches. Hence, Frank (2000, 2007) proposed to assess the conceptual reference models from different views, which are not necessarily independent. This evaluation methodology is partially supported by Recker (2005), although he is focusing on a more paradigmatic evaluation technique where he states that “different philosophical viewpoints determine and impact an artefact construction process, the same can be said about evaluation design” (Recker, 2005, p. 6). The researcher has therefore combined the two researchers’ approaches and formulated the following criteria for the internal evaluation, which are shown in Table 10:

What is the underlying paradigm of the modelling approach? Is it interpretive, positivistic, or constructional?	The underlying assumption was driven by an interpretive and constructional paradigm. The intend of the models is not to reflect ultimate truth, but to capture the general understanding of the EM domain and identify possible improvements.
How good is the relation of a model to reality? Does the model reflect the essential elements?	The models are based on secondary data, case studies, interviews, and observations in the field. Although this is a good basis to reflect reality, each model can only capture a certain part of reality. However, intermediate results halve always been discussed with the participants and improved when necessary
What is the purpose of the model? Is enough information presented to draw a conclusion?	The purpose of the modes was two fold. First, some of the models should give the researcher a better understanding of the processes and organizational structures of the researched organizations. Second, abstracted models should highlight general issues of the domain and identify space for improvement or serve as a reference for EM organizations.
Is the level of abstraction appropriate? Does the model contain the right information in the right quantity and granularity?	From the researcher's view, the granularity and abstraction is appropriate. However, it has to be considered that the researcher knows the whole context to each model. He can therefore only give a biased view. Same is true for the participants of the researched organizations, they know their surrounding and therefore the context of the model. Hence, final judgement can only be made by third parties.
Would a different modelling technique come to the same results?	In some cases BPMN and UML could have been used interchangeably and would yield identical results. However, this was not tested for the generic diagrams which did not follow a standardized modelling language.
Can the model be compared to meta-models? Are their similarities to other models within the same domain which can also relate to the meta-model?	Using meta-models and generic models to compare specific models of the researched organizations was one of the core research methods. Hence, all models of the same type should be comparable.
Is the modelling language chosen appropriate? Does the chosen tool support the correct model types	The mainly utilized modelling tool was ADONIS:CE, since it supports different modelling types and languages (BPNM / UML). The model types were used according to the purpose. In case the researcher needed an more abstract and less formal model to represent ideas or situations he used generic diagrams using MS Visio.

Table 10: Conceptual Referece Model - Evaluation Crititeria

Even though Frank's and Recker's evaluation criteria were used to self-assess the developed concepts, a more objective approach was sought after. First, two of the developed concepts have been applied to the major case-study "MAC2" as an example. This was done to show their applicability in a familiar EM organization. However, since the models and methods could not be applied in real-life and tested over an extended period of time, the researcher chose to use an expert evaluation. According to Fettke, Loos, and Zwicker (2005, p. 9) "only evaluations by third parties ensure the reference models' independency and usability". Thus, the final evaluation was conducted by independent experts in the EM domain. Both forms of evaluation are is described in the following sections.

10.1 Application of the Conceptual Methods

Since the major case-study MAC2 (see chapter 6.2.2, p.126) has shown significant areas of improvement it was chosen to proof the applicability of two of the concepts and present the methods in a more tangible way. The main objective in this stage was to answer the question, if the developed concepts can remedy or at least minimize some of the identified issues of the researched cases. Therefore, IVEM², IT-ORG / CrIO, and ITCO4EM have been assessed accordingly.

10.1.1 IVEM² in Major Case 2

Fist the IVEM² method was assessed since MAC 2 already begun to implement Emergency Modules (see Appendix C (Major Case 2 - Documents), pp.244) for their EM operations. In order to expand their efforts and link their current IT-projects to EM the structure from Figure 51 (p.207) was used and filled with real scenarios, EM modules, and IT-Projects (technologies). Only the layer IT-Services had to be made up. However, given the fact that the researcher knew the organizations demands from EM and IT perspectives and was also aware of the current IT-projects, the IT-services used in this example should be quite realistic. Therefore, the following figure will show the results of IVEM² with data from MAC2.

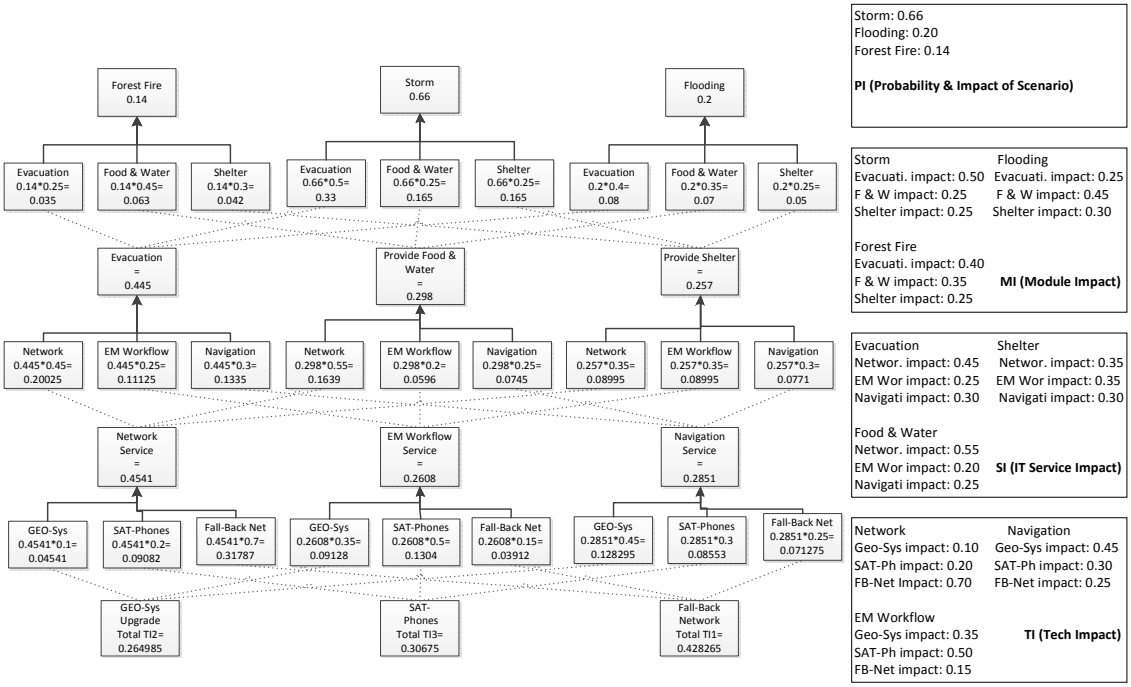


Figure 56: IVEM² in MAC2

The numbers in this case show that MAC2 should favour the "Fall-Back Network" project over the "SAT-Phones" project, and that over the "GEO-Sys Upgrade" project. Compared to some statements from the interviews at MAC2, these IVEM² results reflect the current decisions about IT-investments in MAC2, quite well. Thus, it is concluded that this method would also work in MAC2 when fully implemented.

10.1.2 IT-ORG / CrIO in Major Case 2

One of the major problems of MAC2 is the cooperation between the IT department of the city, the IT department of the EM unit and the EM operations (cp. Chapter 6.2.2, p.126). Hence, the implementation of the IT-ORG / CrIO was discussed with representatives of MAC2 during the interviews and case study. If we look at a snippet of their organizational structure as shown in the following figure one can see that there is a missing link between the IT departments and the EM operations that is able to "translate" between the parties. The only link between all of them is the City Council or Ad-hoc Team. However, both of them do not have the knowledge and oversight to make sustainable IT decisions. Hence, their IT decision archetype (cp. Adapted

version of the Weil & Ross decision matrix, Table 5 (p.159)) tends to be an EM monopoly or IT monopoly rather than a duopoly.

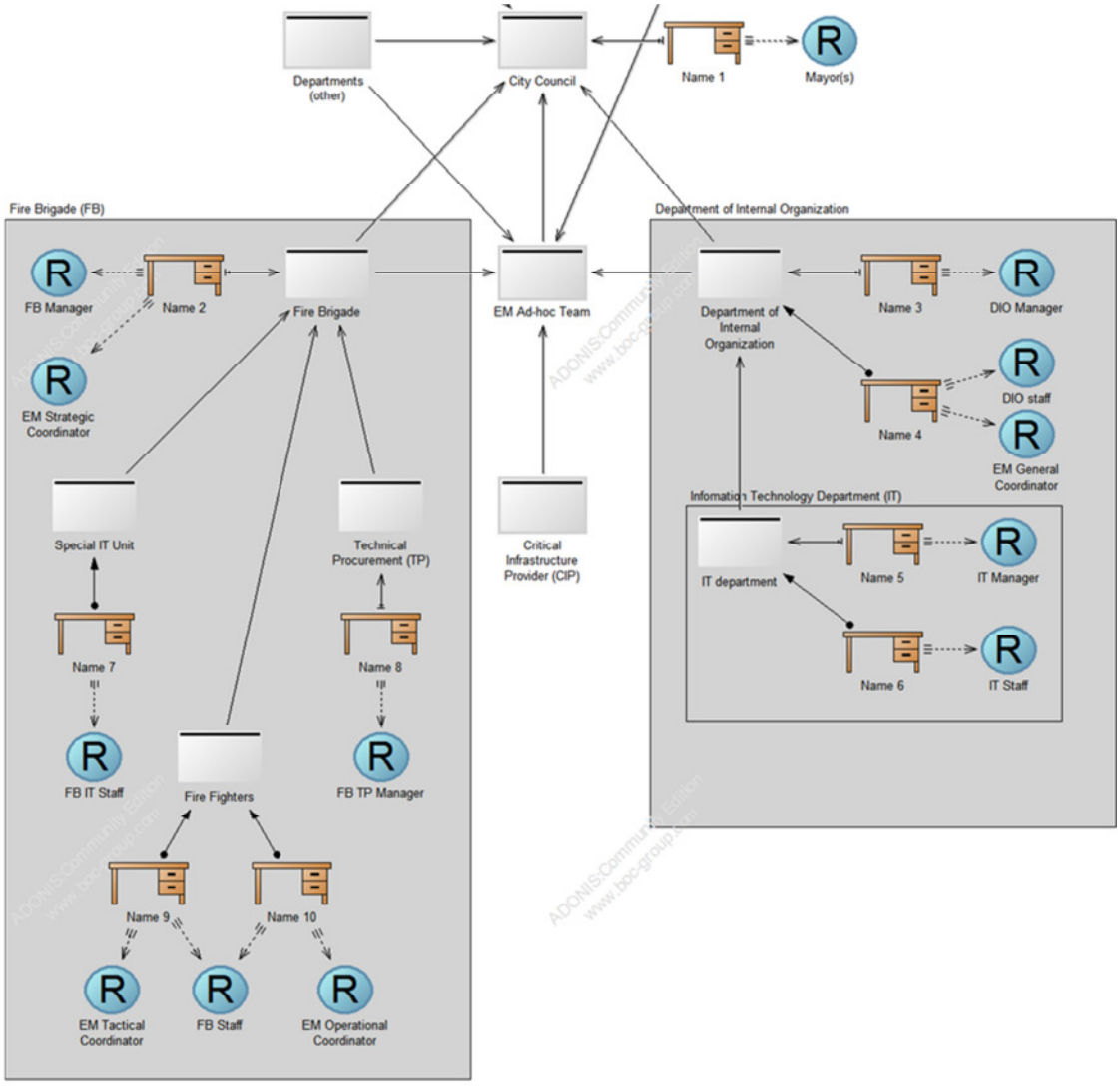


Figure 57: MAC2 Organization Snippet

However, by implementing a CrIO and favouring a duopoly in some decision areas tensions and disagreements can be reduced significantly. A positive example of this would be Major Case 1 that is using IT-Governance committees as a tool to steer their IT decisions. Therefore, it can be said that an organizational structure, such as envisaged with the IT-ORG / CrIO approach, would be able to reduce MAC2 IT decision problems. However, it must be mentioned that some interviewees believed that such an implementation would cause “political tensions” between the parties and will be hard to implement at the current stage.

10.1.3 ITICO4EM in Major Case 2

The ITICO4EM approach could not be implemented with MAC2 in the given timeframe. However, because of the iterative development of the methods participants of MAC2 had a strong influence on the structure of the approach. Particularly the EM operations and EM-IT department were strongly involved in the development process.

One of the most appreciated changes of ITICO4EM in comparison to ITIL or COBIT was its reduced complexity and the strong relation to EM tasks. Therefore, the participants attested the concept a good applicability in EM organization, which currently do not have a strong IT Management. This also reflects some of the findings of the expert evaluation survey, which is described in the following chapter.

10.2 Expert Evaluation – Final Survey

As described in Chapter 5.6 the final survey was conducted online using Google Forms and Google Docs. Therefore, it was completely anonymous and complied with university's ethics guidelines. Participants of the case studies and other interviewees were deliberately excluded from the survey. This was done since the researcher had the feeling this would result in a biased evaluation. Particularly during the case studies the researcher and his project became known to the participants. This resulted in a social relation to some degree that could have influenced their evaluation in positive way, which would affect the result and make the evaluation less valid. Hence, the evaluation form was only sent to communities, forums, and experts, which did not participate in the research project before. This had a positive effect in two ways. Frist, it ensured that the evaluation was not biased, and second that the evaluations was compared to EM organizations and processes, which had not been researched before and, therefore, supported or disproved the applicability of the models and methods.

The demographic data was asked to ensure that the surveys were filled out by experts in the field to ensure the quality and relevance of the answers. During the survey analysis, these data sets were checked to ensure validity of the

submitted surveys. All submitted forms were considered as authentic answers of EM experts. Even though this survey was only submitted by personal invitation and/ or specific channels (ISCRAM / IAEM Newsletter), it cannot be assured that all submissions were filled out by the targeted group. However, since the answers did not show major inconsistencies the researcher sees this as negligible for the outcome of the survey.

The main part of the survey intended to test the EM domain specific IT Governance models and methods (see Chapter 9) in relation to existing methods and processes in the survey participant's organization. The goal is to see in which section the framework is superior or inferior to current solutions. Hence, the survey was based on questions about the applicability, usability, and reliability of the conceptual model and methods. A nine point Likert-scale (Likert, 1932), as described in Chapter 9.3, was used to evaluate the approaches and see if they over or underperform existing processes in other EM organizations. The Likert-scale allowed the researcher to validate his qualitative findings and conceptual models by using quantitative methods.

10.2.1 Final Survey Results

The survey had a return rate of 13 % which is quite normal for an extensive survey in IS research. The evaluation survey and downloads were available for a month as shown in the following diagram. The diagram also reveals that it took most participants quite long to read the documentation, thus most responses came in in the last two weeks of the survey.

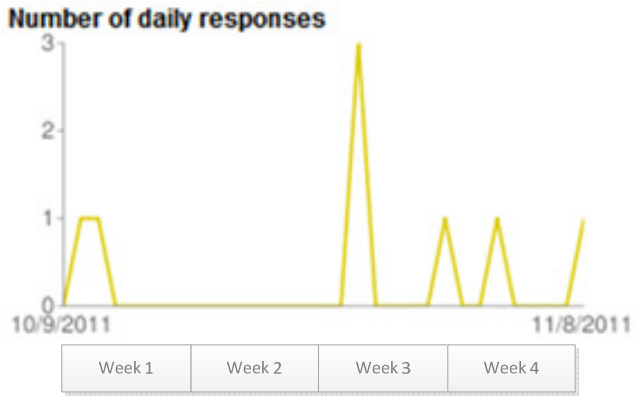


Figure 58: Survey Time Frame and Daily Responses

An interesting finding was that the provided documents have been downloaded from basically every continent, however the most responses came from the USA and Germany.

All participants were between 26 and 55 years old with an average experience in EM of 5-10 years or more. However, the participants' professional background was quite diverse, which reflects the homogenous character of the EM domain. Most participants have been working with large EM organizations and had a good IT and EM knowledge, though some of them had only minor knowledge about IT Governance.

The general feedback of these participants was quite positive as shown in the following diagram.

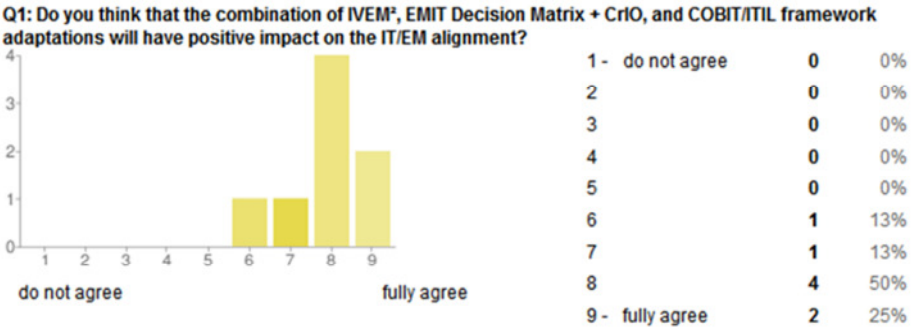


Figure 59: General Feedback on the IT/EM Alignment approaches

However, some weaknesses became evident too. Thus, the following sections are split into strengths and weaknesses of the proposed approaches. Since the complete survey results and statistical values are shown in Appendix H (Evaluation Survey & Results), they will only discuss the most important findings.

10.2.1.1 Strength of the Approaches

The most interesting finding was that medium and large EM organizations are seen as the most appropriate target group for the new approaches, whereas small EM organizations are generally not seen as very suitable.

For example the IVEM² approach, is rated 8 and 9 in large organizations and has an average of 6-7 in medium organizations as shown in the following figures:

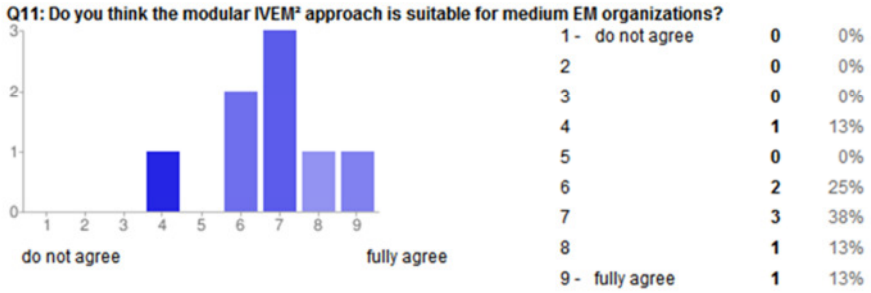


Figure 60: IVEM² Performance in Medium EM Organizations

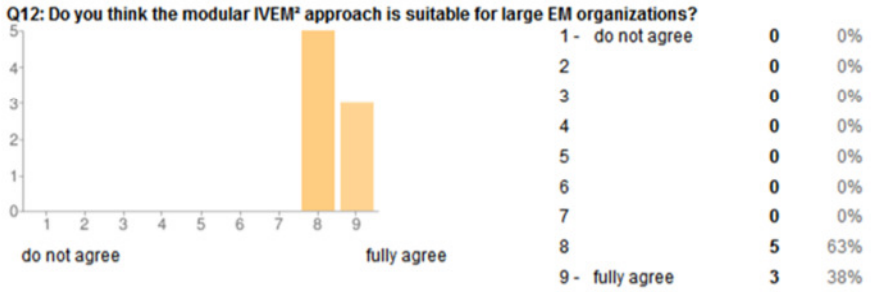


Figure 61: IVEM² Performance in Large EM Organizations

In contrast to medium and large organizations, the IVEM² performance was ranked below average as shown in the next chapter.

An identical behaviour was recognized for IT-ORG /CrIO, as shown in the next two diagrams.

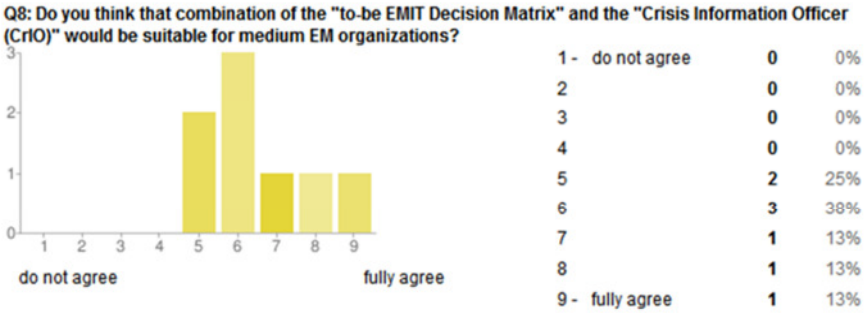


Figure 62: IT-ORG / CrIO Performance in Medium EM Organizations

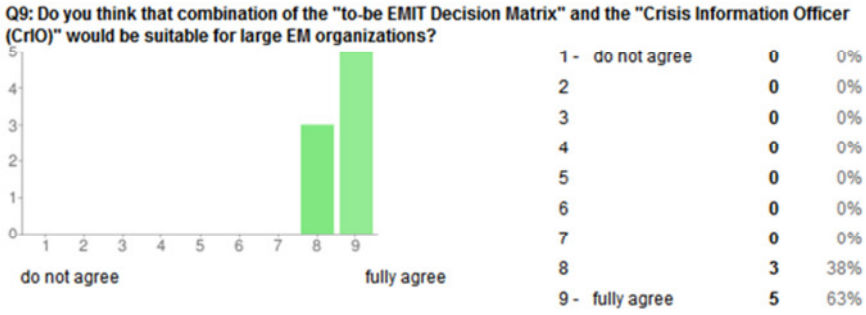


Figure 63: IT-ORG / CrIO Performance in Large EM Organizations

However, it seems as the ITICO4EM approach is, at least to certain degree, also suitable for smaller EM organizations, as the following figures are indicating.

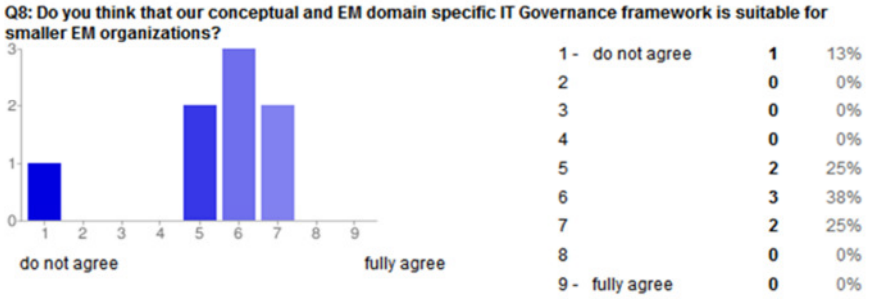


Figure 64: ITICO4EM Performance in Small EM Organizations

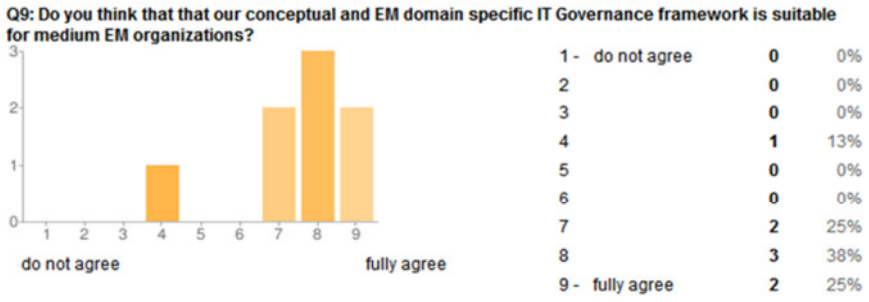


Figure 65: ITICO4EM Performance in Medium EM Organizations

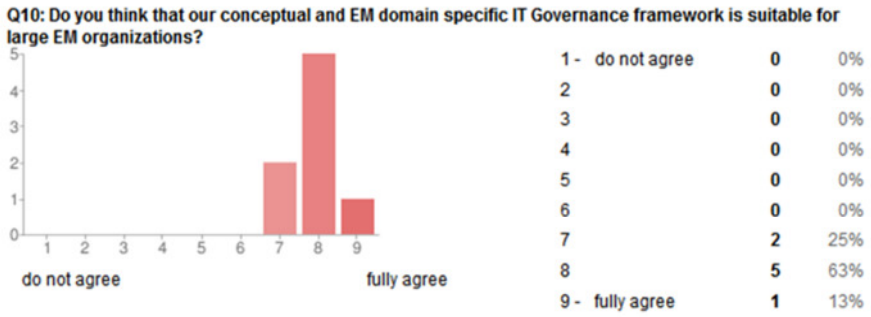


Figure 66: ITICO4EM Performance in Large EM Organizations

As initially said the general feedback was quite positive. However, most interestingly was that the ITICO4EM approach is seen as less complex as other IT Governance and ITSM Frameworks, which was one of the main goals of this research (see Figure 67). Nevertheless, as already mentioned above, it seems as the whole concept is still too complex for small EM organizations. However, the ITICO4EM approach might be a start for them and can be even improved in further research projects.

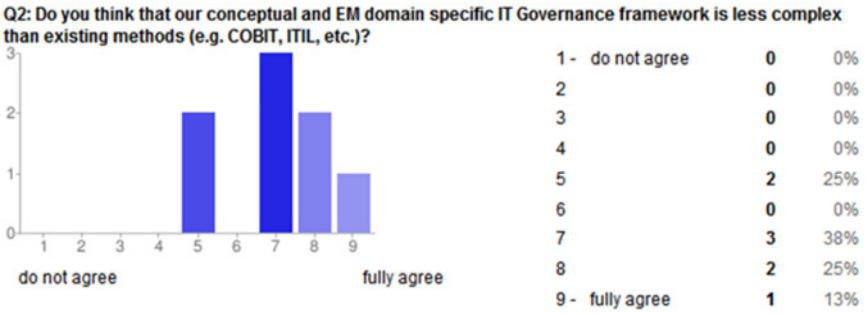


Figure 67: ITICO4EM Complexity Compared to other IT Governance Frameworks

Moreover, all participants attest the ITICO4EM approach that it still covers the most important and relevant aspects, and can address most IT related issues in EM as shown in the following figure.

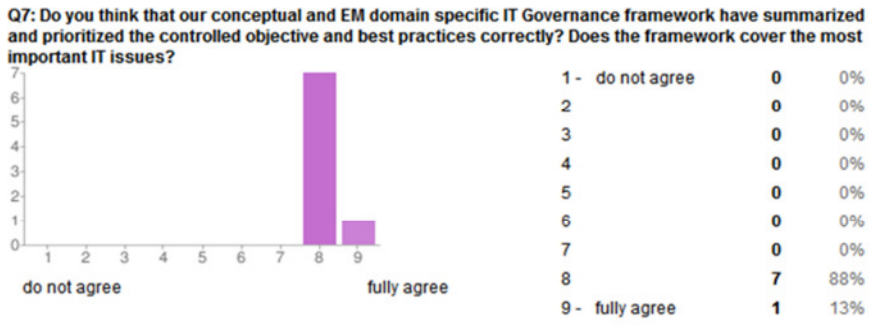


Figure 68: ITICO4EM Aggregation Level

10.2.1.2 Weaknesses of the Approaches

Even though it seems as if the IT Governance approaches have generally a positive effect, particularly in medium to large organizations, they do not fully fit in small EM organizations yet as the following diagrams indicate.

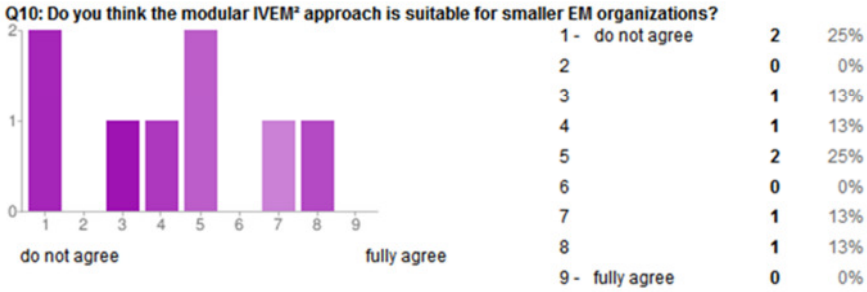


Figure 69: IVEM² Performance in Small EM Organizations

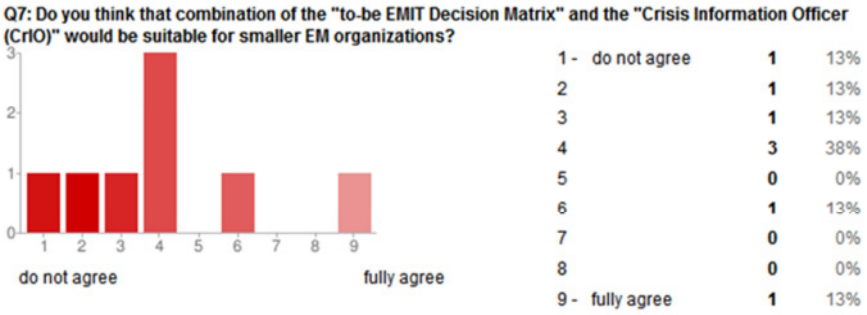


Figure 70: IT-ORG / CrIO Performance in Small EM Organizations

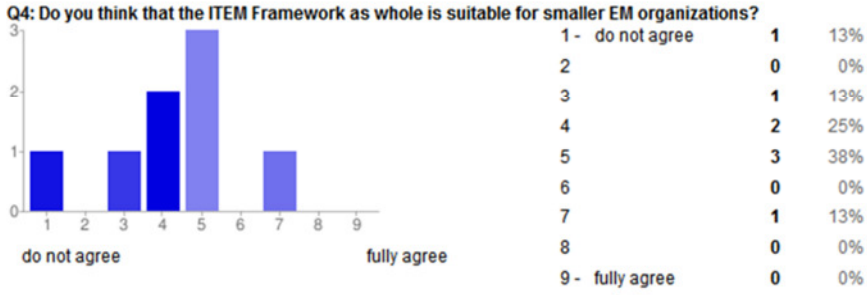


Figure 71: General Performance of the IT/EM Approaches in Small EM Organizations

The only approach, which seems to be applicable in small EM organizations are the ITICO4EM processes. Unfortunately, the participants did not elaborate on the issues of IVEM² and IT-ORG / CrIO, so only assumptions can be made. Therefore, the researcher suggests that this should be investigated in future research projects.

10.3 Discussing the Test Results

Even though an invitation to participate in the survey had been sent out via the newsletters of two large EM communities (the larger one has over 5000 members worldwide), the response to the evaluation survey was unfortunately not as high as anticipated.

It was assumed that around 50 researchers and experts in the field would participate in the survey, but only 62 participants downloaded the evaluation survey, 30 participants downloaded the animated presentation, 14 have downloaded the detailed ITICO4EM processes description, and 13 have downloaded the ITICO4EM mapping. However, only 8 participants have filled out the evaluation survey completely. This is a return rate of 13%, which can be seen as quite normal.

The low participation rate reflects the low IT adoption rate of EM professionals. The invention letter indicated the topic “IT Governance” which might have been a barrier for some EM professionals to even click on the survey link. Another reason could have been that at the same time the survey invitation was sent out, EM professionals were either concerned with the earthquake in Turkey or the ongoing IAEM conference in Munich. However, even a second reminder did not result in a significant increase in responses as the graphs in Appendix H (Evaluation Survey & Results) indicate.

Nevertheless, the final participants have given valuable feedback and generally rated the researcher’s new approaches better than the existing methods and procedures. This indicates the comprehensiveness, pre-eminence, and general applicability of the ITEM-Governance approach in other EM organizations. However, all of the participants agree that even though attempts were made to simplify IT Governance processes, the approach is still too complex for small EM organizations. Therefore, it can be said that the research missed one of its goals to provide an IT Governance method even for the small EM Organizations. Nevertheless, it must be said that none of the existing frameworks, such as ITIL and COBIT, can fulfil this requirement either. Therefore, this remains a yet unsolved issue, which has to be addressed by future research.

PART V:
Conclusion & Recommendations

11 Conclusion

Emergency management plays an important role in today's society. Fast acting first responders and prepared emergency managers are crucial for successful prevention, preparation, response, and relief of all hazardous impacts. IT has proven its potential in industry where it is able to optimize and accelerate processes. However, the domain of Emergency Management is still in its infancy with regard to IT Management and IT Governance. Consequently, they do not create value of their IT initiatives or simply do not use IT since they do not trust in IT enabled processes. Time and reliability are crucial factors in an emergency situation – seconds can decide over life or death. A well-defined and managed IT infrastructure can enable EM organizations to make better and faster decisions. Aligning IT initiatives with Emergency Management objectives can be the key for a more efficient and effective use of information systems.

However, literature and results of an early research stage have identified a lack of proper IT alignment and value creation in the domain of Emergency Management. Even though, there are existing IT Governance methods, which help to improve IT alignment in industry, researchers and Emergency Management professionals jointly agree that the domain of Emergency Management is different and demands methods, which are tailored to its needs. Therefore, the major research question of this thesis was:

How can Strategic IT Alignment in Emergency Management organizations be improved to get most value out of IT initiatives and consequently achieve better emergency preparedness?

To answer this question the researcher conducted a first set of interviews with a focus group in order to identify the most crucial issues with regard to IT Governance and the domain of Emergency Management. Consequently, three underpinning Research questions were formed, which were:

1. ***How can existing IT Governance frameworks and processes help EM organizations to realize and preserve the value of IT initiatives and what adaptations are needed to meet EM specific requirements?***

This question was answered with the ITICO4EM approach. ITICO4EM is a set of simplified and adapted IT Governance and IT Service Management processes, structured in a way to which EM organizations can relate to. It is based on ITIL and COBIT and fully compatible to these frameworks. However, in contrast to ITIL and COBIT it uses EM related terminology and consists only of processes, which are relevant for the domain of EM. The final evaluation survey testified that ITICO4EM is simpler than existing IT Governance frameworks, but still covers all necessary IT issues and can be used in small, medium, and large EM organizations.

2. ***How do EM organizations govern their IT now and what kind of organizational structures and IT decision rights are needed to govern and align IT initiatives effectively?***

During the case studies and interviews it became clear that the organizational structure of EM organizations is different to most other domains. Escalation procedures and inter-organizational collaboration make it difficult for EM organizations to make sustainable IT decisions. Hence, the researcher has analysed the decision making structures and proposed an IT Governance decision matrix, which enables IT and EM to make conjoint decisions within and across departments and organizations. Hence, internal and external IT Governance steering committees are suggested in order to develop a mutual IT vision and to increase the interoperability of information systems, which will ultimately lead to a better information flow. In addition to this, the implementation of a Crisis Information Officer (CrIO) is suggested, who will act as an “ambassador” between IT and EM and can “translate” and “mediate” between the two sides. The IT-ORG / CrIO approach was also positively evaluated for medium and large EM organizations. However, it seems to have deficiencies for smaller organizations, which have to be addressed in future research.

3. ***How can the value of IT initiatives be measured or estimated in uncertain environments in order to establish an IT portfolio of the most valuable IT initiatives?***

The last underpinning research questions has been addressed by IVEM², an IT value estimation method for Emergency Management organizations. During case studies in EM organizations it became evident that rather rigid plans for emergency situations are of limited use for IT related decisions since they are too complex and inflexible. Therefore, this thesis proposes IVEM², a modular approach, which enables EM organizations to align their IT initiatives with uncertain emergency situations and helps them to estimate risk and value of ICT investments more easily. Instead of a conventional emergency plans it uses recurring patterns and processes in the form of modules, which can be flexibly reused like “LEGO stones” in every possible emergency situation. In addition, these smaller “chunks” make it easier for EM personnel to estimate the value and risk of IT initiatives since they are less complex as comprehensive emergency situation descriptions. Therefore, IVEM² was seen as most fruitful for large organizations and medium organizations, but it is also not suitable for smaller EM organizations. This is understandable since an IT portfolio needs a certain dimension. For only two or three IT initiatives, a multi-criteria decision-making method is oversized.

Conclusively it can be said that the research has addressed the initial research questions completely and that the proposed IT Governance approach is showing promising results.

One of the keys factors for the success of this research was the domain specific engineering approach, which enabled the researcher to define the domain’s requirements and needs. By utilizing qualitative and quantitative methods, as well as different modelling techniques the researcher was able to identify barriers and opportunities of existing IT Governance methods and consequently developed domain specific approaches.

Of course, this approach is not a panacea for all EM organizations, but it can give the right impetus for a better utilizations of IT in the domain. Considering the fact that ITIL and COBIT have been developed over decades by multiple researchers and experts, this research project can only be seen as a beginning.

However, the developed methods can be used by other EM organizations as a reference or template to strengthen their IT Governance processes and

ultimately their strategic IT alignment in order to realize more value from their IT investments. A positive example would be the MAC2 case study. Even though, not all elements of the developed method have been implemented until today they have realized that a modular approach, such as used in IVEM², is much more flexible to plan their EM processes and it lays the foundation for a full IVEM² implementation, which would help them to make the right IT investment decisions. Besides that, they have already realized that their organizational structure is not optimal for sustainable IT decisions since there is a missing organizational element that links EM and IT together. Hence, MAC2 would certainly benefit from the developed IT-ORG / CrIO approach as the evaluation has shown. In addition to this, medium sized EM organizations can benefit from the simplified and tailored ITCO4EM framework, since it is less complex than existing IT Governance frameworks such as ITIL and COBIT.

The implementation of these conceptual solutions will be challenging since the domain itself is quite reluctant to change. However, the results are promising and according to the expert evaluation the developed approaches have a high chance to add valuable merit to society and the domain of EM.

12 Future Research and Limitations

The domain of Emergency Management is quite small compared to industry and not very well researched in terms of IT in general, and IT Governance in particular, which limited the available and relevant scientific resources for this research project. Additionally, most EM organizations have sensitive data and are reluctant to make them available to outsiders. As a result, this research is only based on a few researched organizations and interviews. Because of this, one can argue that the results are not generally applicable to all EM organizations. However, the researcher tried to minimize these shortcomings by incorporating a maximum of variety of EM organizations and conducted his research in an international setting.

Because of their critical functions, research in EM organizations is often limited to a conceptual stage, including this project. Even though, the researcher tried to work as closely with experts as possible and observed a large pandemic drill under “real-life” conditions, the results of this research are only at a conceptual stage. Nevertheless, the research project is showing promising results, which have been supported by an expert evaluation survey. However, only future research can show how the approaches will perform in action. Hence, the researcher suggests the following directions for future research.

The final evaluation survey showed that small EM organizations still have problems to utilize some of the proposed methods. Hence, the researcher suggests that future research should investigate in this area. In a parallel research project about IT Service Management in small and medium enterprises (SME) it was realized that most micro-companies in industry have difficulties to manage and align their IT too. Maybe, a cross-domain research project can shed light on this issue.

Due to financial limitations and time constraints, the researcher did not implement any maturity models and detailed implementation guidelines in this project. Nevertheless, it is strongly encouraged that future research should focus on this issue. Even though the approaches are tailored towards the requirements of the researched domain, some organization might have

difficulties implementing them. Moreover, it became evident that the majority of organizations in the domain of EM are quite “change reluctant” and particularly IT related innovations are seen sceptically. It is the researcher’s belief that this “change reluctance” could be remedied by are more detailed implementation guideline, which should include a suitable maturity model and a change management approach that ensures the support of all stakeholders.

Finally, since the project’s focus was to develop conceptual models, a ‘proof of concept in real-life’ is still missing. Even though, the final evaluation, has shown promising results the concepts need to be tested and improved under conditions that are more realistic. One of the researched cases has already started to define reusable modules for their EM operations since they have realized they will become more efficient and flexible in multiple emergency situations. However, the strategic use of IT is still not implemented in their concept. This case would be an ideal candidate to test the developed “ITEM Governance” approach, and to refine and improve its concepts. Therefore, the researcher would like to encourage not only this particular organization to support future research projects, but also other EM organizations that face the same problems.

PART VI:
Appendix and Bibliography

13 Appendix A (Interview Questionnaire)

- Questionnaire:

Demographic Data:

Position/Function:

Sector (Governance / NGO / Private)

Geographic Location:

Size of Organization:

Questions to your Organization:

1. Do you have a Corporate Strategy?
   - If "Yes" what are your top 10 strategic goals?
   - If "No" why don't you have a Corporate Strategy and what / who (no real names, just the business function) guides your business decisions?
2. Do you have an ICT Governance body?
   - If "Yes" what ICT governance Frameworks are you using and how is your process maturity? Did you make adaptations to those frameworks? If "yes", explain them and give reasons.
   - If "No" why don't you have an ICT Governance body and on what are your ICT decisions based instead? Is there reason that you don't use ICT Governance frameworks?
3. Please fill out the following matrix, put in the functions/business units who give input and who decide:

IT Gov Tasks (left-right) / IT Gov Archtypes (top-down)		Define IT Strategy		Define IT Architecture		Maintain IT Infrastructure		Defining IT Services for Operations		IT Investmens	
		IT	EM	IT	EM	IT	EM	IT	EM	IT	EM
Business Monarchy	is										
	be										
IT Monarchy	is										
	be										
EM Feudal	is										
	be										
Federal	is										
	be										
Duopoly	is										
	be										
Anarchy	Is										
	be										
No Data / Don't know	is										
	be										

*If you chose "other" please describe your governance structure briefly

4. Do you think the allocation of input /decision is optimal in this matrix? If not, what should be changed?
5. Briefly explain your organizational diagram and describe the major tasks of the important units for EM processes. How does your ICT unit fit in?
6. Explain your sourcing strategy (e.g. in-sourcing, out-sourcing, etc.) for your ICT unit. Why did you choose that sourcing strategy and what are the major advantages /disadvantages?
7. How do you measure the overall performance of your ICT unit?

Questions to your operational processes:

8. Please describe your major EM processes and important day-to-day processes
9. Does your organization use ICT for in EM processes?
    - If “yes”, why was the decision made to implement and use such systems?
    - If “no”: why do you not use such systems
10. Are you satisfied with your ICT solutions?
    - If “yes” why you are satisfied (examples)?
    - If “no” what should be improved?
11. Give examples of EM situations of which you think your ICT didn’t support you or other involved parties sufficiently. Why do you think that happened?

Questions to ICT:

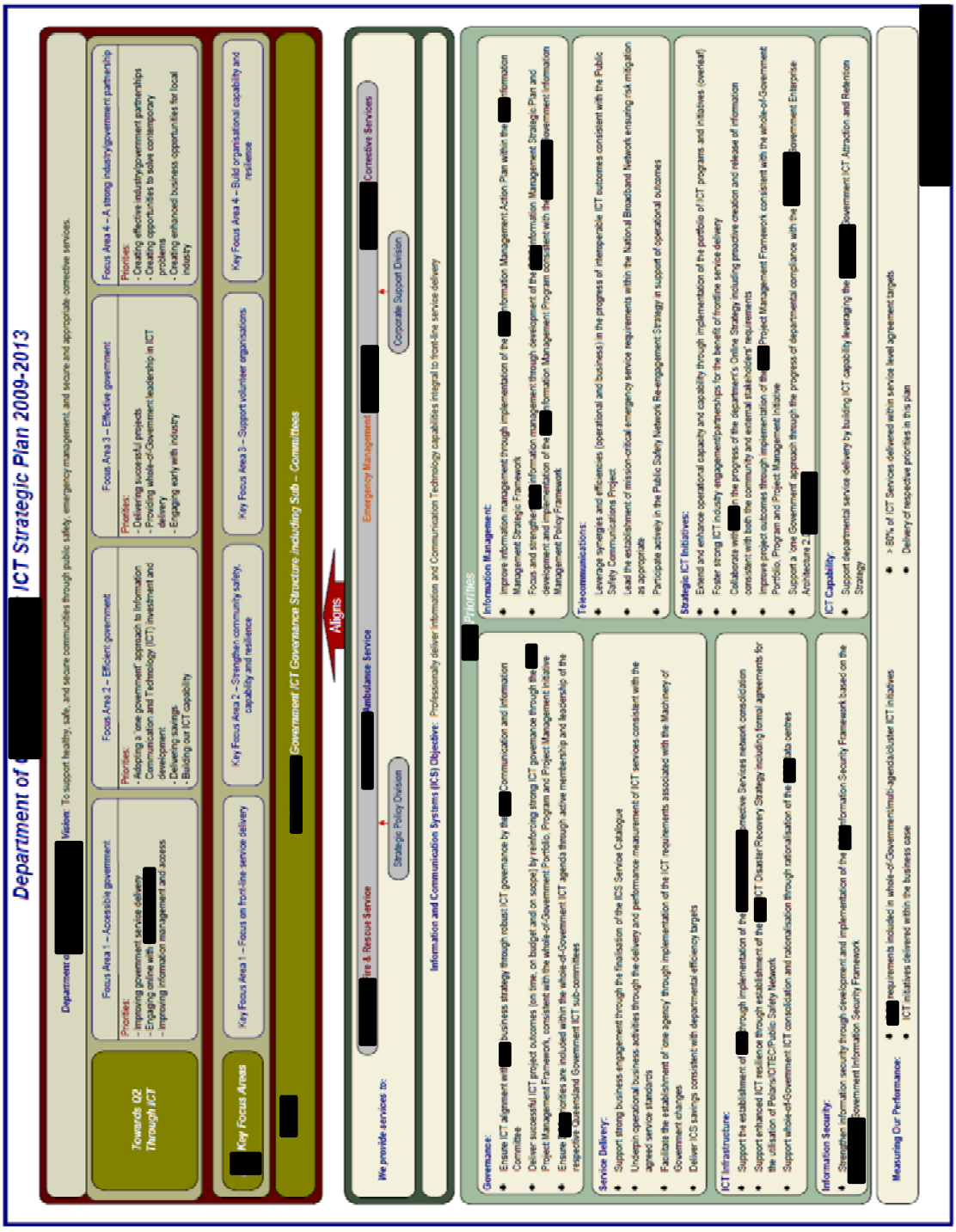
12. Explain your EM related ICT processes briefly.
13. How do you define your ICT requirement specifications?
14. Describe your ICT purchase process briefly.
15. Do you think your ICT unit does understand your needs and do they fully support you?
    - If “yes” explain how you communicate your needs
    - If “no” why do you think they don’t understand your needs or why do you think they don’t give you full support
16. Do you think your ICT unit does inform you about new ICT systems that might be beneficial to EM processes?
    - If “yes” how and do they inform you and how frequently?
    - If “no” what are the reason they don’t inform you?
17. Is your ICT unit actively involved in the design of EM processes?
    - If “yes” why are they involved?
    - If “no” why are they not involved?
18. Do you think your Emergency Managers understand the opportunities and risks of new ICT systems and are they able to improve their processes with such systems?
    - If “yes” how do they do it?
    - If “no” why do you think they are not aware of those factors?

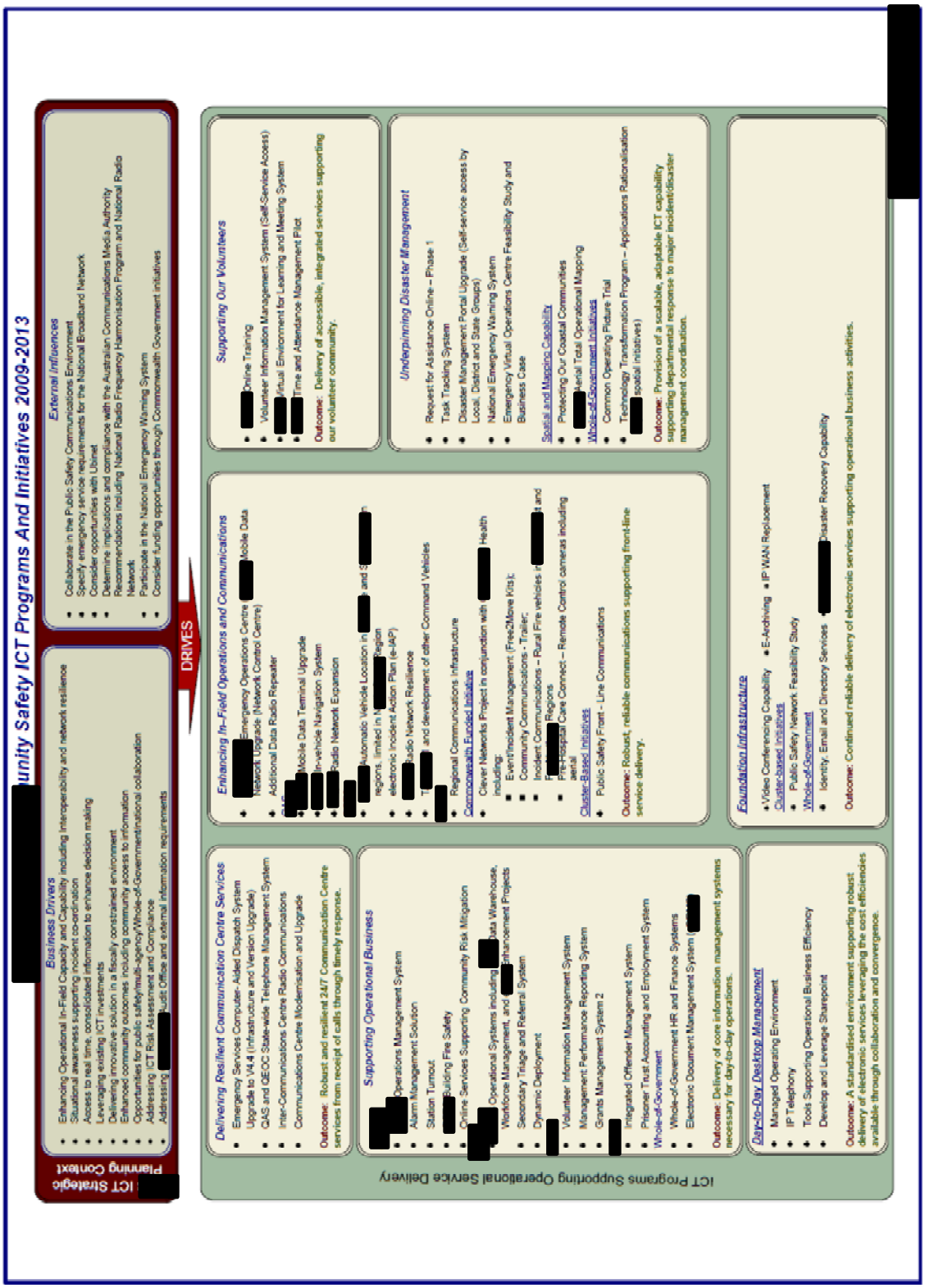
19. Is your ICT architecture for EM processes independent or is it integrated into a larger enterprise architecture. Why is that so and do you think that is a good solution?
20. Are all systems and services known, which are involved in EM processes and are Service Levels clear and appropriate?
    - If “yes”, how is it done and how frequently are they revised?
    - If “no”, why is that so? Wouldn’t it be better if all systems and services are known and SLAs are clear and appropriate?
21. Are your systems and services designed under an ICT architecture and are they well integrated and interoperable or do you have “information isles”?
    Explain why?
    Would you change it if you could and what would that change look like?
22. How do you incorporate the different phases of a disaster into your ICT “strategy”? Which phase is the most important to you and why? Which are the second and third and why?
23. Do you measure your ICT in regard to
    a. Impact / Value
    b. Risk
    c. Performance
    d. Reliability
    e. Security
        - If “yes” how do you do it?
        - If “no” why don’t you do it?
24. Does your ICT impact and risk analysis incorporate “unpredictable” scenarios or are your decision based on fixed scenarios?
    - If “yes” explain how your impact / risk analysis deals with such uncertainties
    - If “no”, do you think a more flexible impact and risk analysis would be advantageous for your processes and budgeting?
25. Do your ICT investments compete with conventional investments or do they have their own budgeting? Explain why you have chosen that approach.
26. Do you have an ICT investment/project portfolio?
    - If “yes” how does it look like? How is your strategic, tactical and operational mix?
        - What are the factors for prioritization?
    - If “no” why don’t you make use of such portfolio?
        - If you had to create a portfolio, what would the factors for prioritization be?

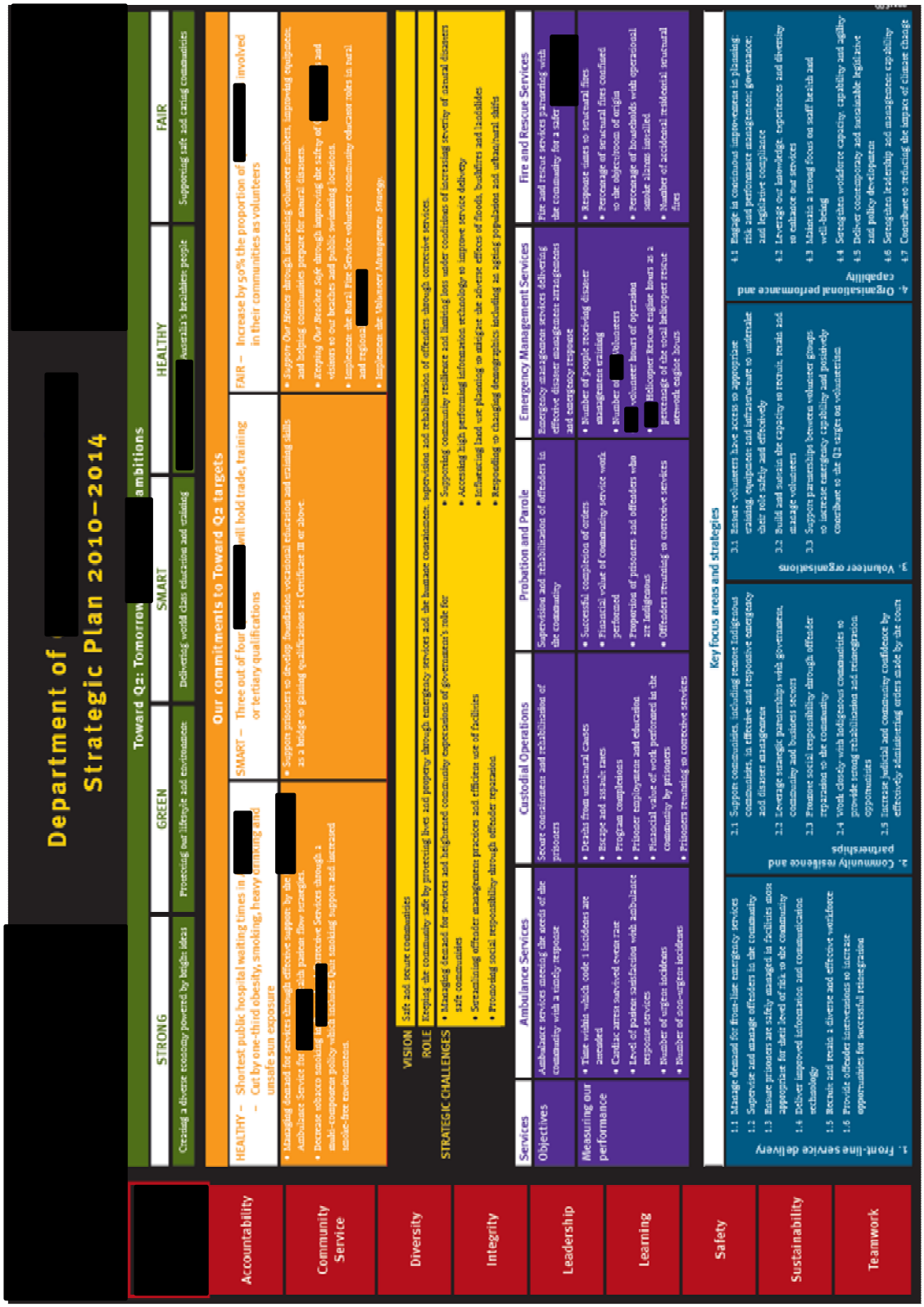
Questions “Other”:

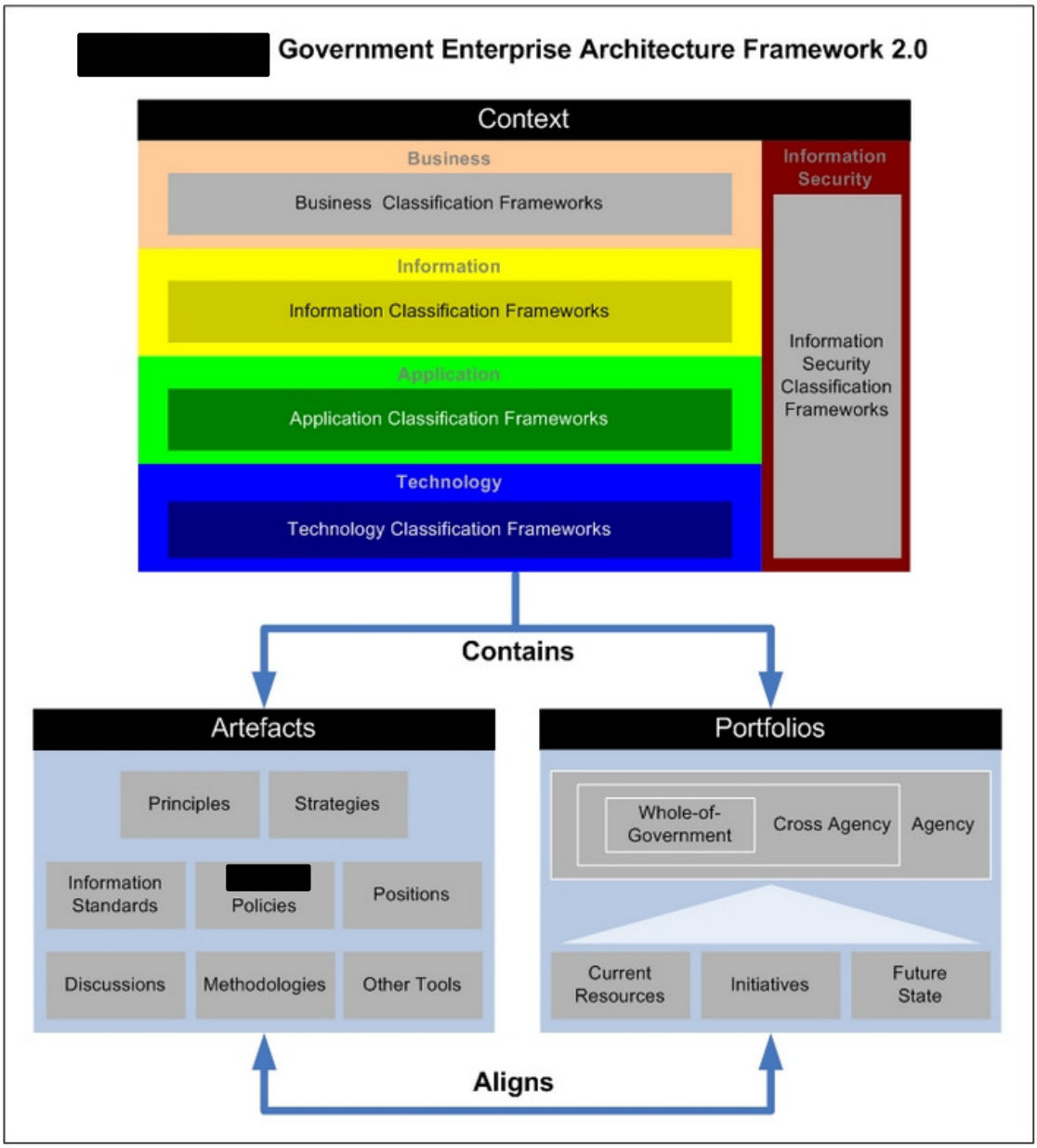
27. Are there other issues or processes (not covered by the previous sections) which are important to you or your organization? Describe them briefly or give examples.

14 Appendix B (Major Case 1 - Documents)

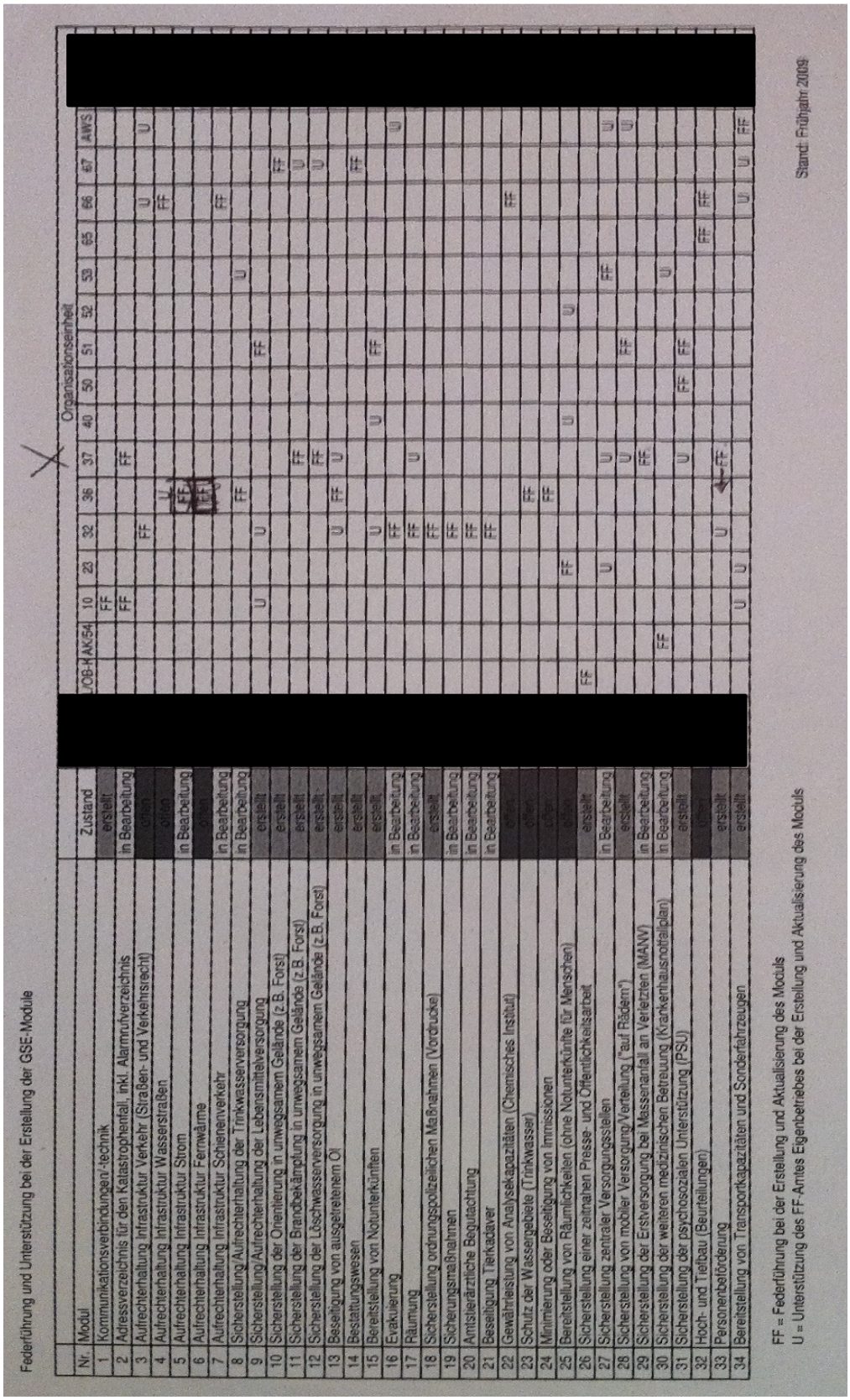



unity Safety ICT Programs And Initiatives 2009-2013
ICT Strategic Planning Context
Business Drivers
Enhancing Operational In-Field Capability and Capability including interoperability and network resilience
Situational awareness supporting incident coordination
Access to real time, consolidated information to enhance decision making
Leveraging existing ICT investments
Delivering innovative solution in a fiscally constrained environment
Enhanced community outcomes including community access to information
Opportunities for public safety/multi-agency/Whole-of-Government/national collaboration
Addressing ICT Risk Assessment and Compliance
Addressing [redacted] Audit Office and external information requirements
External Influences
Collaborate in the Public Safety Communications Environment
Specify emergency service requirements for the National Broadband Network
Consider opportunities with Ubinet
Determine implications and compliance with the Australian Communications Media Authority Recommendations including National Radio Frequency Harmonisation Program and National Radio Network
Participate in the National Emergency Warning System
Consider funding opportunities through Commonwealth Government initiatives
DRIVES
ICT Programs Supporting Operational Service Delivery
Delivering Resilient Communication Centre Services
Emergency Services Computer- Aided Dispatch System Upgrade to V4.4 (Infrastructure and Version Upgrade)
QAS and QEOC State-wide Telephone Management System
Inter-Communications Centre Radio Communications
Communications Centre Modernisation and Upgrade
Outcome: Robust and resilient 24/7 Communication Centre services from receipt of calls through timely response.
Supporting Operational Business
[redacted] Operations Management System
Alarm Management Solution
Station Turnout
[redacted] Building Fire Safety
Online Services Supporting Community Risk Mitigation
[redacted] Operational Systems including [redacted] Data Warehouse, Workforce Management, and [redacted] Enhancement Projects
Secondary Triage and Referral System
Dynamic Deployment
[redacted] Volunteer Information Management System
Management Performance Reporting System
Grants Management System 2
[redacted] Integrated Offender Management System
Prisoner Trust Accounting and Employment System
Whole-of-Government
Whole-of-Government HR and Finance Systems
Electronic Document Management System ([redacted])
Outcome: Delivery of core information management systems necessary for day-to-day operations.
Day-to-Day Desktop Management
Managed Operating Environment
IP Telephony
Tools Supporting Operational Business Efficiency
Develop and Leverage Sharepoint
Outcome: A standardised environment supporting robust delivery of electronic services leveraging the cost efficiencies available through collaboration and convergence.
Enhancing In-Field Operations and Communications
[redacted] Network Upgrade (Network Control Centre)
Additional Data Radio Repeater
[redacted] Mobile Data Terminal Upgrade
In-vehicle Navigation System
Radio Network Expansion
[redacted] Automatic Vehicle Location in [redacted] regions, limited in N[redacted] Region
electronic Incident Action Plan (e-IAP)
Radio Network Resilience
T[redacted] and development of other Command Vehicles
Regional Communications Infrastructure
Commonwealth Funded Initiative
Clever Networks Project in conjunction with [redacted] Health including:
Event/Incident Management: (Free2Move Kits);
Community Communications – Trailer;
Incident Communications – Rural Fire vehicles in [redacted] and Fire Regions
Fire-Hospital Care Connect – Remote Control cameras including aerial
Cluster-Based Initiatives
Public Safety Front – Line Communications
Outcome: Robust, reliable communications supporting front-line service delivery.
Supporting Our Volunteers
[redacted] Online Training
Volunteer Information Management System (Self-Service Access)
[redacted] Virtual Environment for Learning and Meeting System
[redacted] Time and Attendance Management Pilot
Outcome: Delivery of accessible, integrated services supporting our volunteer community.
Underpinning Disaster Management
Request for Assistance Online – Phase 1
Task Tracking System
Disaster Management Portal Upgrade (Self-service access by Local, District and State Groups)
National Emergency Warning System
Emergency Virtual Operations Centre Feasibility Study and Business Case
Spatial and Mapping Capability
Protecting Our Coastal Communities
[redacted] Aerial Total Operational Mapping
Whole-of-Government Initiatives
Common Operating Picture Trial
Technology Transformation Program – Applications Rationalisation
[redacted] spatial initiatives)
Outcome: Provision of a scalable, adaptable ICT capability supporting departmental response to major incident/disaster management coordination.
Foundation Infrastructure
Video Conferencing Capability
E-Archiving
IP WAN Replacement
Cluster-based Initiatives
Public Safety Network Feasibility Study
Whole-of-Government
Identity, Email and Directory Services
[redacted] Disaster Recovery Capability
Outcome: Continued reliable delivery of electronic services supporting operational business activities.


Department of [redacted]
Strategic Plan 2010–2014
Toward Q2: Tomorrow [redacted] ambitions
STRONG
Creating a diverse economy powered by bright ideas
GREEN
Protecting our lifestyle and environment
SMART
Delivering world class education and training
HEALTHY
[redacted] Australia's healthiest people
FAIR
Supporting safe and caring communities
Our commitments to Toward Q2 targets
HEALTHY – Shortest public hospital waiting times in [redacted]
– Cut by one-third obesity, smoking, heavy drinking and unsafe sun exposure
SMART – Three out of four [redacted] will hold trade, training or tertiary qualifications
FAIR – Increase by 50% the proportion of [redacted] involved in their communities as volunteers
• Managing demand for services through effective support by the Ambulance Service for [redacted] with patient flow strategies.
• Decrease tobacco smoking in [redacted] Corrective Services through a multi-component policy which includes Quit smoking support and increased smoke-free environment.
• Supports prisoners to develop foundation vocational education and training skills as a bridge to gaining qualifications at Certificate III or above.
• Supports Our Heroes through increasing volunteer numbers, improving equipment and helping communities prepare for natural disasters.
• Keeping Our Beaches Safe through improving the safety of [redacted] and visitors to our beaches and public swimming locations.
• Implements the Rural Fire Service volunteer community educator roles in rural and regional [redacted]
• Implements the Volunteer Management Strategy.
VISION Safe and secure communities
ROLE Keeping the community safe by protecting lives and property through emergency services and the humane containment, supervision and rehabilitation of offenders through corrective services.
STRATEGIC CHALLENGES
• Managing demand for services and heightened community expectation of government's role for safe communities
• Streamlining offender management processes and efficient use of facilities
• Promoting social responsibility through offender reparation
• Supporting community resilience and limiting loss under conditions of increasing severity of natural disasters
• Accessing high performing information technology to improve service delivery
• Influencing land use planning to mitigate the adverse effects of floods, bushfires and landslides
• Responding to changing demographics including an ageing population and urban/rural shifts
Services
Ambulance Services
Custodial Operations
Probation and Parole
Emergency Management Services
Fire and Rescue Services
Objectives
Ambulance services meeting the needs of the community with a timely response
Secure containment and rehabilitation of prisoners
Supervision and rehabilitation of offenders in the community
Emergency management services delivering effective disaster management arrangements and emergency response
Fire and rescue services partnering with the community for a safer [redacted]
Measuring our performance
• Time within which code 1 incidents are attended
• Cardiac arrest survived event rate
• Level of patient satisfaction with ambulance response services
• Number of urgent incidents
• Number of non-urgent incidents
• Deaths from unnatural causes
• Escape and assault rates
• Program completions
• Prisoner employment and education
• Financial value of work performed in the community by prisoners
• Prisoners remaining in corrective services
• Successful completion of orders
• Financial value of community service work performed
• Proportion of prisoners and offenders who are Indigenous
• Offenders returning to corrective services
• Number of people receiving disaster management training
• Number of [redacted] volunteers
• [redacted] volunteer hours of operation
• [redacted] helicopter rescue [redacted] as a percentage of the total helicopter rescue network neglect hours
• Response times to structural fires
• Percentage of structural fires confined to the object/room of origin
• Percentage of households with operational smoke alarms installed
• Number of accidental residential structural fires
Key focus areas and strategies
1. Front-line service delivery
1.1 Manage demand for front-line emergency services
1.2 Supervise and manage offenders in the community
1.3 Ensure prisoners are safely managed in facilities appropriate for their level of risk to the community
1.4 Deliver improved information and communication technology
1.5 Retain and recruit a diverse and efficient workforce
1.6 Provide offender interventions to increase opportunities for successful reintegration
2. Community resilience and partnerships
2.1 Support communities, including remote Indigenous communities, in effective and responsive emergency and disaster management
2.2 Leverage strategic partnerships with government, community and business sectors
2.3 Promote social responsibility through offender reparation to the community
2.4 Work closely with Indigenous communities to provide strong rehabilitation and reintegration opportunities
2.5 Increase judicial and community confidence by effectively administering orders made by the court
3. Volunteer organisations
3.1 Retain volunteers have access to appropriate training, equipment and infrastructure to undertake their role safely and effectively
3.2 Build and sustain the capacity to recruit, retain and manage volunteers
3.3 Support partnerships between volunteer groups to increase emergency capability and positively contribute to the Q2 target on volunteering
4. Organisational performance and capability
4.1 Engage in continuous improvement in planning, risk and performance management, governance, and legislative compliance
4.2 Leverage our knowledge, experience and diversity to enhance our services
4.3 Maintain a strong focus on staff health and well-being
4.4 Strengthen workforce capacity, capability and agility
4.5 Deliver contemporary and sustainable legislative and policy development
4.6 Strengthen leadership and management capability
4.7 Contribute to reducing the impact of climate change
Accountability
Community Service
Diversity
Integrity
Leadership
Learning
Safety
Sustainability
Teamwork


[redacted] Government Enterprise Architecture Framework 2.0
Context
Business
Business Classification Frameworks
Information
Information Classification Frameworks
Application
Application Classification Frameworks
Technology
Technology Classification Frameworks
Information Security
Information Security Classification Frameworks
Contains
Artefacts
Principles
Strategies
Information Standards
[redacted]
Policies
Positions
Discussions
Methodologies
Other Tools
Portfolios
Whole-of-Government
Cross Agency
Agency
Current Resources
Initiatives
Future State
Aligns

15 Appendix C (Major Case 2 - Documents)



Federführung und Unterstützung bei der Erstellung der GSE-Module

Nr.	Modul	Zustand	[redacted]	UOB-HAK/54	10	23	32	36	37	40	Organisationseinheit 50	51	52	53	65	66	67	AWS
1	Kommunikationsverbindungen/-technik	erstellt			FF													
2	Adressverzeichnis für den Katastrophenfall, inkl. Alarmrufverzeichnis	in Bearbeitung			FF				FF									
3	Aufrechterhaltung Infrastruktur Verkehr (Straßen- und Verkehrsrecht)	offen					FF									U		U
4	Aufrechterhaltung Infrastruktur Wasserstraßen	offen						U								FF		
5	Aufrechterhaltung Infrastruktur Strom	in Bearbeitung						FF										
6	Aufrechterhaltung Infrastruktur Fernwärme	offen						FF										
7	Aufrechterhaltung Infrastruktur Schienenverkehr	in Bearbeitung														FF		
8	Sicherstellung/Aufrechterhaltung der Trinkwasserversorgung	in Bearbeitung						FF						U				
9	Sicherstellung/Aufrechterhaltung der Lebensmittelversorgung	erstellt			U		U		U			FF					FF	
10	Sicherstellung der Orientierung in unwegsamem Gelände (z.B. Forst)	erstellt															FF	
11	Sicherstellung der Brandbekämpfung in unwegsamem Gelände (z.B. Forst)	erstellt							FF								U	
12	Sicherstellung der Löschwasserversorgung in unwegsamem Gelände (z.B. Forst)	erstellt							FF								U	
13	Beseitigung von ausgetretenem Öl	erstellt					U	FF	U									
14	Bestattungswesen	erstellt															FF	
15	Bereitstellung von Notunterkünften	erstellt					U			U		FF						
16	Evakuierung	in Bearbeitung					FF		U									U
17	Räumung	in Bearbeitung					FF		U									
18	Sicherstellung ordnungspolizeilichen Maßnahmen (Vordrucke)	erstellt					FF											
19	Sicherungsmaßnahmen	in Bearbeitung					FF											
20	Amtsärztliche Begutachtung	in Bearbeitung					FF											
21	Beseitigung Tierkadaver	in Bearbeitung					FF											
22	Gewährleistung von Analysekapazitäten (Chemisches Institut)	offen														FF		
23	Schutz der Wassergebiete (Trinkwasser)	offen						FF										
24	Minimierung oder Beseitigung von Immissionen	offen						FF										
25	Bereitstellung von Räumlichkeiten (ohne Notunterkünfte für Menschen)	erstellt				FF				U			U					
26	Sicherstellung einer zeitnahen Presse- und Öffentlichkeitsarbeit	erstellt		FF														
27	Sicherstellung zentraler Versorgungsstellen	in Bearbeitung				U			U					FF				U
28	Sicherstellung von mobiler Versorgung/Verteilung ("auf Rädern")	erstellt							U			FF						U
29	Sicherstellung der Erstversorgung bei Massenanfall an Verletzten (MANV)	in Bearbeitung							FF									U
30	Sicherstellung der weiteren medizinischen Betreuung (Krankenhausnotfallplan)	in Bearbeitung		FF										U				
31	Sicherstellung der psychosozialen Unterstützung (PSU)	erstellt							U		FF	FF						
32	Hoch- und Tiefbau (Beurteilungen)	offen													FF	FF		
33	Personenbeförderung	erstellt					U		FF									
34	Bereitstellung von Transportkapazitäten und Sonderfahrzeugen	erstellt			U	U										U	U	FF

FF = Federführung bei der Erstellung und Aktualisierung des Moduls
U = Unterstützung des FF-Amtes Eigenbetriebes bei der Erstellung und Aktualisierung des Moduls

Stand: Frühjahr 2009

	Module:																																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Sturm / Orkan Tornado (3111)			x					x	x				x														x	x						x	
Blitzeis / Eisregen (3112)			x		x																							x	x						
Langanhaltender Schneefall / Schneeverwehungen (3113)	x				x	x	x	x						x	x	x												x						
Langanhaltender Starkfrost (3114)									x																			x			x				
Hitze und Dürreperioden mit Trinkwassermangel (3117)								x														x				x	x	x						x	
SMOG (3118)			x												x	x							x			x	x	x						x	
Erdbeben (3120)	x		x		x			x	x			x	x	x	x	x			x					x										x	
Erdrutsch (3131)	x		x		x			x	x				x	x	x	x										x	x	x						x	
Waldbrand (3140)	x												x	x	x	x			x							x	x	x						x	
Örtliche Hochwasser nach Starkregen (3152)			x		x			x	x			x				x	x		x							x								x	
Hochwasser in Bächen, Flüssen und Stromtälern (3153)			x		x	x	x	x	x			x			x	x	x		x				x			x	x	x						x	
Meteoriteneinschlag (3160)	x		x		x			x	x				x	x	x	x			x				x			x	x	x						x	
Freisetzung A-Stoffe KKW Inland (3211)								x	x				x	x	x	x										x	x	x						x	
Freisetzung A-Stoffe KKW Frankreich/Schweiz 3212)								x	x						x	x	x									x	x	x						x	
Seuchen (Epedemien z.B.:Influenza u. Pandemien) (3221)								x	x						x	x	x									x	x	x						x	
Tierseuchen (Epizootien) (3222)					x			x							x	x	x									x	x	x						x	
Freisetzung pathogener Stoffe (3224)								x	x							x	x			x	x						x							x	
Freisetzung toxischer Stoffe (3231)								x	x						x	x	x				x					x	x	x						x	
Gefahrstofffreisetzung bei Transprtunfällen (3240)								x	x						x	x	x				x					x	x	x						x	
Gefahrstofffreisetzung bei Öl/Pipelines (3241)								x	x												x	x				x	x	x						x	
Explosionen von Gasbehältern (3245-1)									x		x				x							x				x	x							x	
Explosionen von Mineralöllager (3245-1)									x		x				x											x	x	x						x	
Verkehrsunfall auf der Straße (3251)			x						x																	x	x	x						x	
Schiffsunfall auf Wasserstraßen (3253)					x							x											x			x	x								
Massenanfall von Betroffenen (3255)			x		x	x	x	x	x				x													x	x	x							
Kritische Infrastruktur - Versorgung Gas (3263)					x	x	x	x	x						x	x	x									x	x	x	x	x				x	
Störungen und Schäden in Einrichtungen der Entsorgung:									x						x	x	x									x	x								
Abwassernetze, Klärwerke (3271)					x			x	x																	x	x							x	
Bombenfund (3295)	x				x				x						x											x	x							x	
Terrorismus, Anschläge, Attentate, Sabotage (3300)	x		x		x			x	x				x	x	x				x							x	x							x	

[redacted]

Stand: 15. April 2010

Verwaltungsgliederungsplan und allgemeine Stellvertretung des Oberbürgermeisters

Oberbürgermeister [redacted]

Ständiger allgemeiner Stellvertreter des Oberbürgermeisters

[redacted]

Unmittelbar nachgeordnet	Geschäftskreis Oberbürgermeister: Persönliches Referat	Geschäftskreis Oberbürgermeister: Referat Koordination und Planung	Geschäftskreis I: Referat Allgemeine Verwaltung und Krankenhäuser	Geschäftskreis II: Referat Wirtschaft, Finanzen und Beteiligungen	Geschäftskreis III: Referat Sicherheit und Ordnung	Geschäftskreis III: Rechtsreferat	Geschäftskreis IV: Referat Kultur, Bildung und Sport	Geschäftskreis V: Referat Soziales, Jugend und Gesundheit	Geschäftskreis VI: Referat Städtebau und Umwelt	Geschäftskreis VII: Technisches Referat
[redacted]										
14 Rechnungsprüfungsamt **OB/82** Abteilung Wirtschaftsförderung **OB-KG** Abteilung für individuelle Chancengleichheit von Frauen und Männern	**L/OB-B** Ideen- und Beschwerdemanagement **L/OB-K** Abteilung Kommunikation **L/OB-IM** Abteilung Außenbeziehungen **L/OB-PRE** Abteilung Protokoll, Empfänge und Ehrungen **L/OB-BIP** [redacted] schaft	**S-IP** Abteilung Integration **S-KP** Abteilung Querschnittsaufgaben - Kinderbüro - Mobilität	**10** Haupt- und Personalamt **15** Bezirksämter **AK/AM** Arbeitsmedizinischer Dienst **AK/ISB** Behördlicher Beauftragter für Datenschutz und IT-Sicherheit **AK/SI** Arbeitssicherheitstechnischer Dienst **AK/54** Ref. Abt. Krankenhausbetrieb **KS** Eigenbetrieb Klinikum [redacted]	**20** Stadtkämmerei **23** Amt für Liegenschaften und Wohnen **BBS** Eigenbetrieb Bäderbetriebe [redacted]	**12** Statistisches Amt **32** Amt für öffentliche Ordnung **37** Branddirektion **RSO/KKP** Sicherheitspartnerschaft in der Kommunalen Kriminalprävention	**30** Rechtsamt **34** Standesamt	**40** Schulverwaltungsamt **41** Kulturamt **52** Sportamt **KBS/B.E.** Stabsstelle Bürgerschaftliches Engagement	**50** Sozialamt **51** Jugendamt **53** Gesundheitsamt **ELW** Eigenbetrieb Leben und Wohnen	**36** Amt für Umweltschutz **61** Amt für Stadtplanung und Stadterneuerung **63** Baurechtsamt	**62** Stadtmessungsamt **65** Hochbauamt **66** Tiefbauamt mit **SES** Eigenbetrieb Stadtentwässerung **67** Garten-, Friedhofs- und Forstamt **AWS** Eigenbetrieb Abfallwirtschaft Stuttgart **TVV-I** Ref.-Abt. Verkehrsausbau und Investitionen

[redacted]

Verwaltungsstab (VwS)
Anlage 7

[redacted]

Nachrichtenausgang über Nachrichtensammelstelle

Stand: 30. Dezember 2005

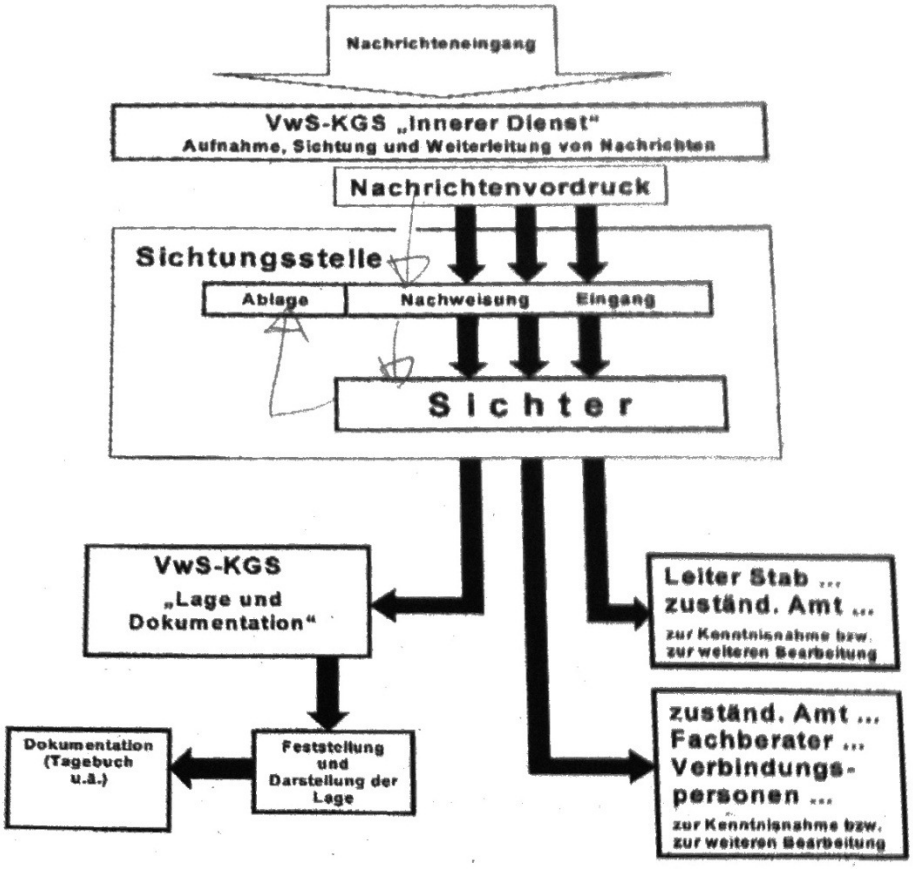
Verwaltungsstab (VwS)
Anlage 7

[redacted]

Informationsfluss

An dieser Stelle wird der gezielte Informationsfluss in, aus und innerhalb den / dem / des Verwaltungsstabes dargestellt. Unabhängig von einer Systementscheidung wird hier die letzte Ausfallebene – nämlich der von Hand auszufüllende Nachrichtenvordruck – in seiner Systematik erläutert.

Nachrichteneingang über Nachrichtensammelstelle



Stand: 30. Dezember 2005

Verwaltungsstab (VwS)
Anlage 6
Erreichbarkeit des Stabes
An dieser Stelle wird ein Kommunikationsplan abgebildet, der alle möglichen Kommunikationswege zwischen den beteiligten Stellen abbildet.
Kommunikationsplan
Stabsgruppe des Verwaltungsstabes (VwS-SGr) oder Verwaltungsstab (VwS)
Bürgertelefon
(Technische) Einsatzleitung
Integrierte Leitstelle Stuttgart
Führungs- und Lagezentrum
vor Ort (inkl. Führungsunterstützung)
rückwärtig
Stand: 30. Dezember 2005

[redacted]

Meldung / Information

Führungsstab / FüS S2+S3 / FüS S5 zu S2

M/I

Einsatz-Nr.:	[redacted]
Einsatzort:	
Einsatztyp:	
Betreff:	AW: Mittelanforderung
Datum:	04.08.2007 **Uhrzeit:** 12:44
Typ:	- **Priorität:** -

Aufnahmevermerk:
- ☒ -
- ○ Bote
- ○ Fax
- ○ Funk
- ○ Mail
- ○ Telefon

Von: FüS - S2 Lage (BelgeGe)	**Absender:** -
An Funktion(en): Einsatzleitung	**Cc Funktion(en):** FüS - Nachweisung; FüS - S2 Lage

3 Löschzüge nachalarmiert

LZ 2, 3
FF Abt. 32

---Ursprüngliche Meldung---
Von: Einsatzleitung
Gesendet: 04.08.2007 12:39
Betreff: Mittelanforderung

Benötigen weiteren Löschzug

Bearbeitungsvermerk ☐

Gedruckt von Einsatzleitung (rlu) am 04.08.2007 um 12:46 Seite 1 von 1

Ausgedruckte Meldung

Rundschreiben Nr. [redacted]

1. Beigeordnete und Referenten
2. Amtsleiterinnen und Amtsleiter
3. Betriebsleitungen der Eigenbetriebe [redacted]

nachrichtlich:
4. Gesamtpersonalrat Verwaltung
5. IuK-Koordinatorinnen und -Koordinatoren
   - nach besonderem Verteiler -

Informations- und Kommunikationstechnik (IuK);
Großschadensereignisse Modul 01: Aufrechterhaltung/Sicherstellung der IuK;
hier: Sicherheitsmaßnahmen für die dezentralen Serverstandorte der Fachämter und Eigenbetriebe

[redacted]

Um bei Großschadensereignissen die Sicherheit der städtischen IuK gewährleisten zu können, ist es u. a. erforderlich, die zentralen und dezentralen Serverstandorte zu überprüfen. Die Basis hierfür bilden das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik und das städtische IT-Sicherheitskonzept [redacted]

Die Server der folgenden Organisationseinheiten sind in den beiden zentralen Serverstandorten untergebracht, sie werden durch die Abteilung Informations- und Kommunikationstechnik (IuK) des Haupt- und Personalamts administriert und überwacht: OB und Referate, Gemeinderat und Fraktionen, Gesamtpersonalrat Verwaltung, 10, 12, 14, 15, 22, 23, 30, 32, 34, 36 (Abt. Energiewirtschaft), 41 (außer 41-3), 50, 51, 52, 53, 65, [redacted] museum, [redacted]

Die Überprüfung dieser Standorte wurde bereits zentral durch die Abt. IuK veranlasst. Basierend auf den Ergebnissen der Überprüfung werden ggf. ergänzende Maßnahmen zur Aufrechterhaltung der Sicherheit durchgeführt, anschließend wird eine zentrale und lückenlose Dokumentation erstellt.

Die Server der folgenden Ämter und Eigenbetriebe sind dezentral untergebracht und werden von diesen selbst betreut: 20, 36, 37, 40, 41-3, 61, 62, 63, 66, 67, [redacted] Aus gegebenem Anlass (erhöhte Gefährdungslage während der [redacted] wird darauf hingewiesen, dass die Unterbringung den o. a. Anforderungen (IT-Grundschutzhandbuch bzw. IT-Sicherheitskonzept) genügen muss und dass dies in der Verantwortung des jeweiligen Fachamts/Eigenbetriebs liegt.

...

Die Untersuchung der folgenden Punkte ist von herausgehobener Bedeutung:

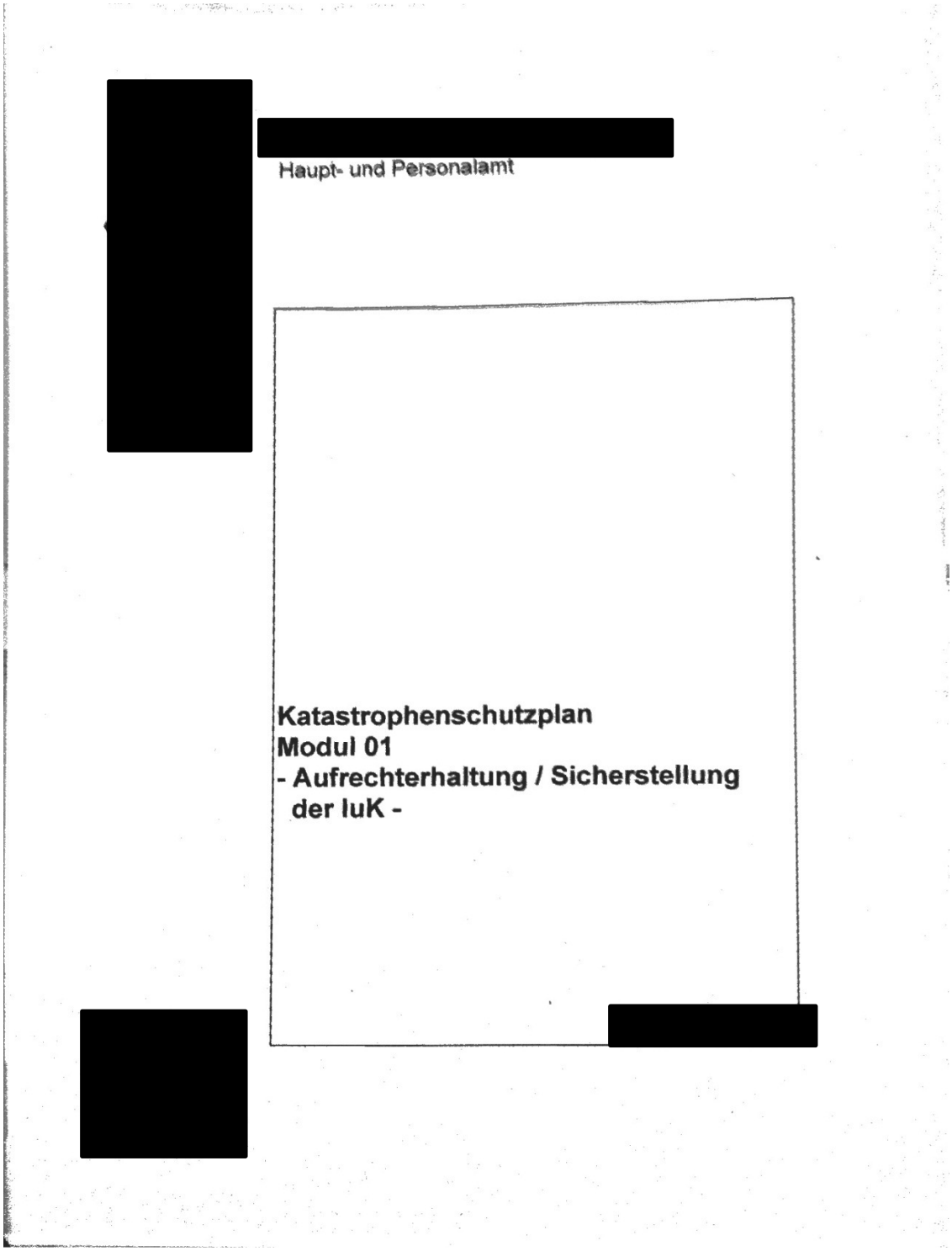
- **bauliche** Voraussetzungen (Klimatisierung, Hochwasserschutz, Brandschutz, unterbrechungsfreie Stromversorgung ...),
- **technische** Voraussetzungen (Dokumentation der Server und der darauf laufenden Anwendungen und Daten, Verkabelung ...),
- **organisatorische** Voraussetzungen (Alarmierungspläne, Lagepläne, Listen mit Know-how-Trägern und Verantwortlichen ...).

Bitte sorgen Sie im Rahmen Ihrer o. g. Verantwortung dafür, dass potenzielle Gefährdungen rechtzeitig und wirkungsvoll abgewendet werden können. Bei Bedarf kann Sie die Abteilung IuK des Haupt- und Personalamts bei Untersuchungen und Umsetzungsmaßnahmen beraten.

Der behördliche Datenschutzbeauftragte kann im Rahmen seines Aufgabengebiets jederzeit auch unangekündigte Kontrollen – gerade auch im Hinblick auf die Umsetzung der o. g. Maßnahmen für die Sicherheit von Serverräumen – durchführen.

gez.

[redacted]


[redacted]
Haupt- und Personalamt
Katastrophenschutzplan
Modul 01
- Aufrechterhaltung / Sicherstellung
der IuK -
[redacted]
[redacted]

[redacted]

Modul 01

Zusammenfassung

- Aufrechterhaltung / Sicherstellung der IuK -

Kurzbeschreibung/Definition

Im Ereignisfall ist die Informations- und Kommunikationstechnik der [redacted] stadt aufrechtzuerhalten. Die Kommunikationswege zw. dem jeweiligen Lage- und Führungszentrum und den Ämtern und Eigenbetrieben müssen sichergestellt werden.

Zuständigkeiten

- Haupt- und Personalamt, Abteilung IuK, für:
  - zentral betreute Hard- und Software
  - Netzwerkmanagement
  - Kontakte zu [redacted]
- Stadtkämmerei, Amt für Umweltschutz, Branddirektion, Schulverwaltungsamt, Kulturamt (Stadtbücherei), Amt für Stadtplanung und Stadterneuerung, Stadtmessungsamt, Baurechtsamt, Tiefbauamt, Garten- und Friedhofsamt, EB Abfallwirtschaft und EB Leben und Wohnen für
  - Eigene, dezentral betreute Hard- und Software

Anmerkung:
Für die Aufrechterhaltung / Sicherstellung der IuK werden keine gesonderten Szenarien erstellt, da es sich um eine im Rahmen des Katastrophenschutzes zu erledigende Querschnittsaufgabe handelt. Allein aufgrund eines Ausfalls der städtischen IuK wird kein Katastrophenfall ausgerufen, sondern auf einen Ausfall der IuK ist im Rahmen eines höherrangigen Großschadensereignisses (z.B. Stromausfall) mit übergeordneten Szenarien und dort zu regelnden weiteren Aspekten zu reagieren.

Liste der wichtigsten Telefon-Nummern:	[redacted]
Leiter Abt. Informations- und Kommunikationstechnik	
Stellvertreter	
IuK-Hotline	

[redacted]

[redacted]

I. 2 Zuständigkeiten und Ansprechpartner

I. 2.1 Zentral: Haupt- und Personalamt, Abt. IuK

Die Abteilung Informations- und Kommunikationstechnik (IuK) administriert und überwacht die Server und Speicherressourcen der folgenden Organisationseinheiten:

- OB und Referate
- Gemeinderat und Fraktionen
- Gesamtpersonalrat Verwaltung
- Haupt- und Personalamt
- Statistisches Amt
- Rechnungsprüfungsamt
- Bezirksämter
- Steueramt
- Amt für Liegenschaften und Wohnen
- Rechtsamt
- Amt für öffentliche Ordnung
- Standesamt
- Amt für Umweltschutz (Abt. Energiewirtschaft)
- Kulturamt (außer Stadtbücherei)
- Sozialamt
- Jugendamt
- Sportamt
- Gesundheitsamt
- Hochbauamt
- Kunstmuseum
- Kur- und Bäderbetriebe Stuttgart.

Die Server dieser Organisationseinheiten sind in den beiden zentralen Serverstandorten Rathaus und [redacted] Gebäude untergebracht.

Ferner werden von der Abt. IuK u. a folgende zentrale Dienste geleistet:

- Netzwerkmanagement für das [redacted]
- Zentraler Mailservice
- Zentrale Datenbankadministration (DB/2, Oracle, MySQL, PostgreSQL, Lotus Notes)
- Sprachkommunikation
- Internet-Zugang
- IuK-Hotline
- IuK-Beratung
- Entwicklung
- Betreuung von Hard- und Software für die o. a. Organisationseinheiten

[redacted]

Modul 01

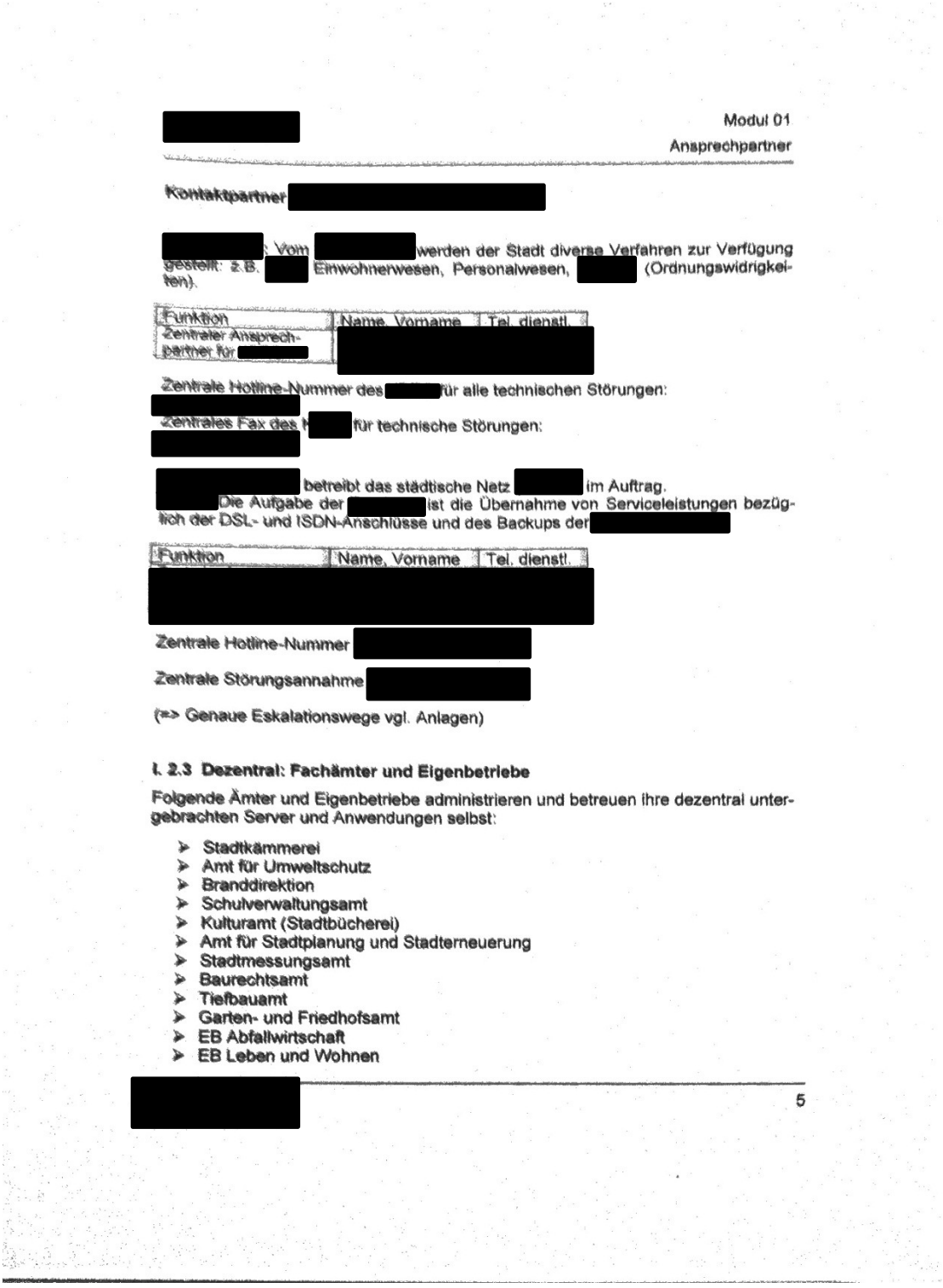
Ansprechpartner

I. 2.2 Ansprechpartner IuK

Funktion	Name, Vorname	Tel. dienstl.	Mobil-Tel.	Privat-Tel.
Abteilungsleiter	[redacted]			
Teamleiter Anwender- und Systemservice				
System- Netzwerkmanagement				
Netzwerkplanung, Sicherheit, Telekommunikation				
UNIX, Netzwerkmanagement				
Windows-Server, SAN				
Web-Server, Firewall, Internet				
Lotus Notes-Administration				
Datenbank-Administration				
Rathaus-Team				
[redacted]				
Betreuung				

[redacted]

4



[redacted]

Modul 01

Ansprechpartner

Kontaktpartner [redacted]

[redacted]: Vom [redacted] werden der Stadt diverse Verfahren zur Verfügung gestellt: z.B. [redacted] Einwohnerwesen, Personalwesen, [redacted] (Ordnungswidrigkeiten).

Funktion	Name, Vorname	Tel. dienstl.
Zentraler Ansprechpartner für [redacted]	[redacted]	

Zentrale Hotline-Nummer des [redacted] für alle technischen Störungen:
[redacted]

Zentrales Fax des [redacted] für technische Störungen:
[redacted]

[redacted] betreibt das städtische Netz [redacted] im Auftrag.
Die Aufgabe der [redacted] ist die Übernahme von Serviceleistungen bezüglich der DSL- und ISDN-Anschlüsse und des Backups der [redacted]

Funktion	Name, Vorname	Tel. dienstl.
[redacted]		

Zentrale Hotline-Nummer [redacted]

Zentrale Störungsannahme [redacted]

(=> Genaue Eskalationswege vgl. Anlagen)

I. 2.3 Dezentral: Fachämter und Eigenbetriebe

Folgende Ämter und Eigenbetriebe administrieren und betreuen ihre dezentral untergebrachten Server und Anwendungen selbst:

- Stadtkämmerei
- Amt für Umweltschutz
- Branddirektion
- Schulverwaltungsamt
- Kulturamt (Stadtbücherei)
- Amt für Stadtplanung und Stadterneuerung
- Stadtmessungsamt
- Baurechtsamt
- Tiefbauamt
- Garten- und Friedhofsamt
- EB Abfallwirtschaft
- EB Leben und Wohnen

[redacted]

5

[redacted]

An den Verwaltungsstab
der
Stadt [redacted]

[redacted]

Pandemieübung [redacted]

Zeitraum der Lage:
26.06. - 06.07. [redacted]

Einspielzeit der Lagemeldung:
07.07. [redacted]

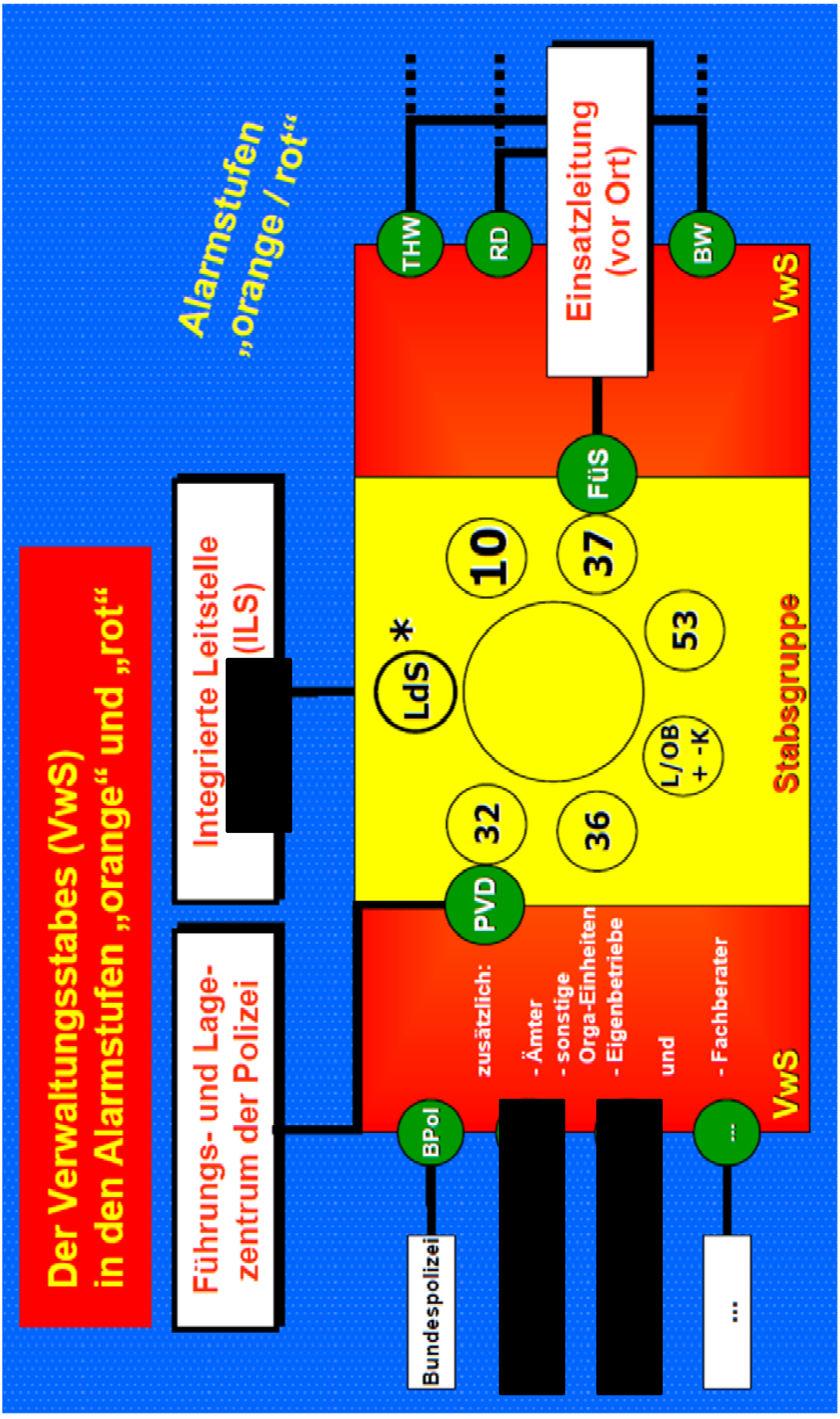
Weltweit : Stand: 06.Juli [redacted]	Weltweit sind 75.256.321 bestätigte Krankheitsfälle in 89 Staaten gemeldet worden. Die Pandemie erfasst Afrika.
Deutschland: Stand: 06.Juli [redacted]	In Deutschland sind es derzeit 7.531.256 bestätigte Krankheitsfälle. Mittlerweile verlagert sich die Pandemie auch in den [redacted] Deutschlands.
[redacted] Stand: 06.Juli [redacted]	In [redacted] sind 4.317.876 Krankheitsfälle gemeldet. Auch der [redacted] ist nun stark betroffen.
[redacted] Stand: 06.Juli [redacted]	In [redacted] sind 121.958 Krankheitsfälle gemeldet, das Gesundheitsamt geht von einer hohen Dunkelziffer aus und schätzt Vorsichtig die reale Zahl derzeit auf 180.000- 200.000 Krankheitsfälle. Vermehrt kommt es zu einer Lebensmittelknappheit. Der bisherige Verlauf entspricht dem erwarteten Verlauf der zu Beginn der Pandemie prognostiziert wurde.

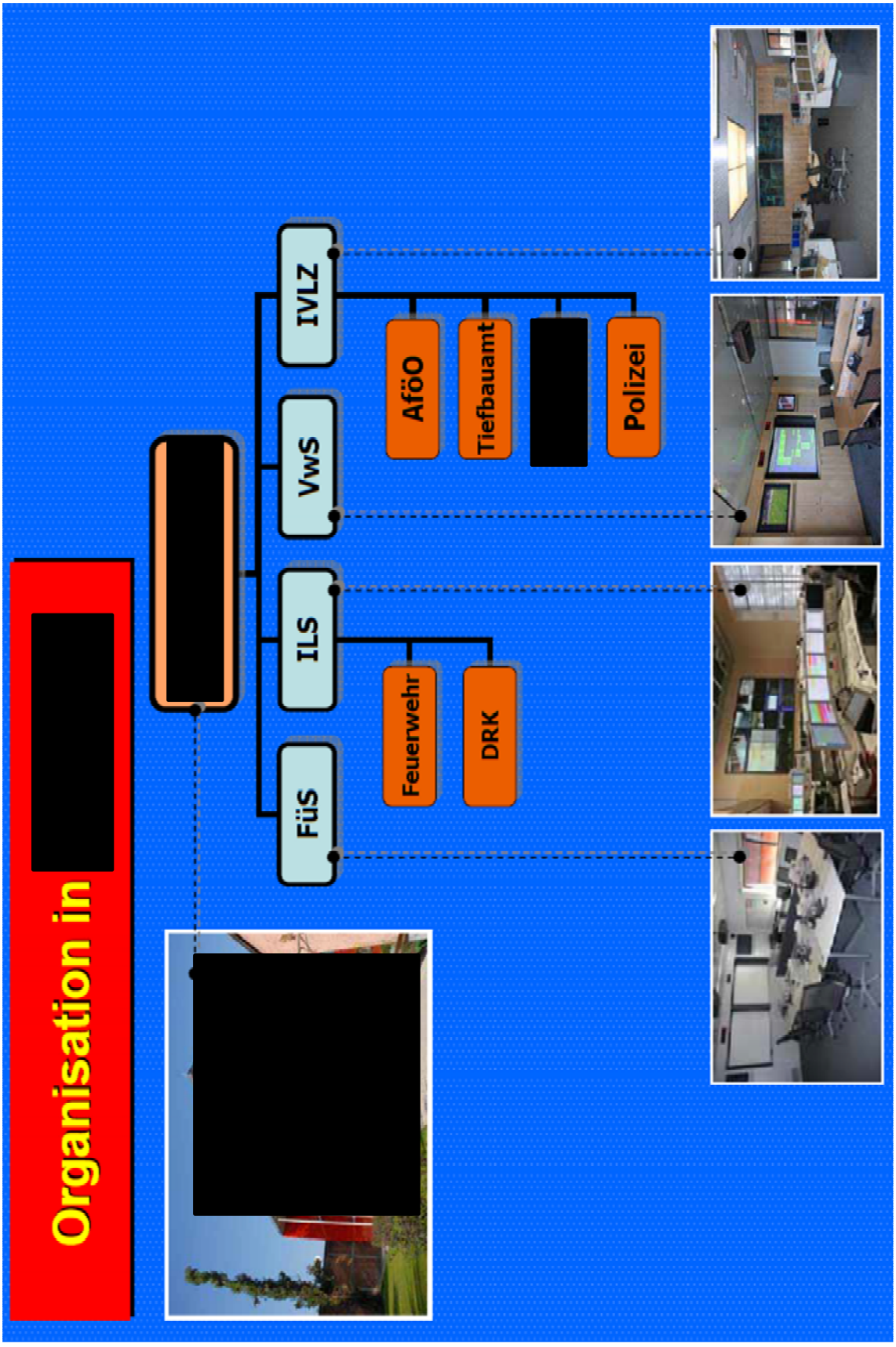
[redacted]

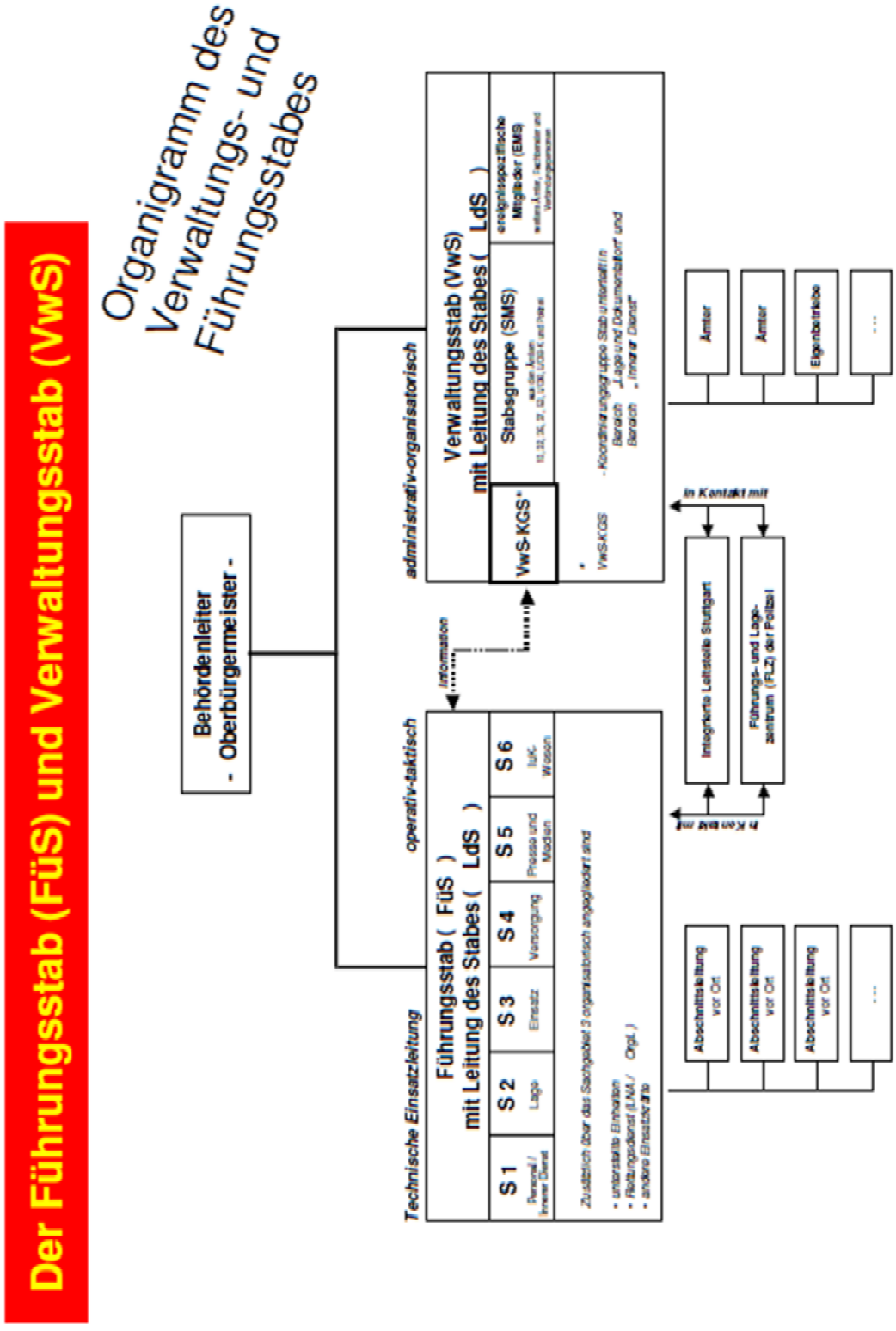
[redacted]

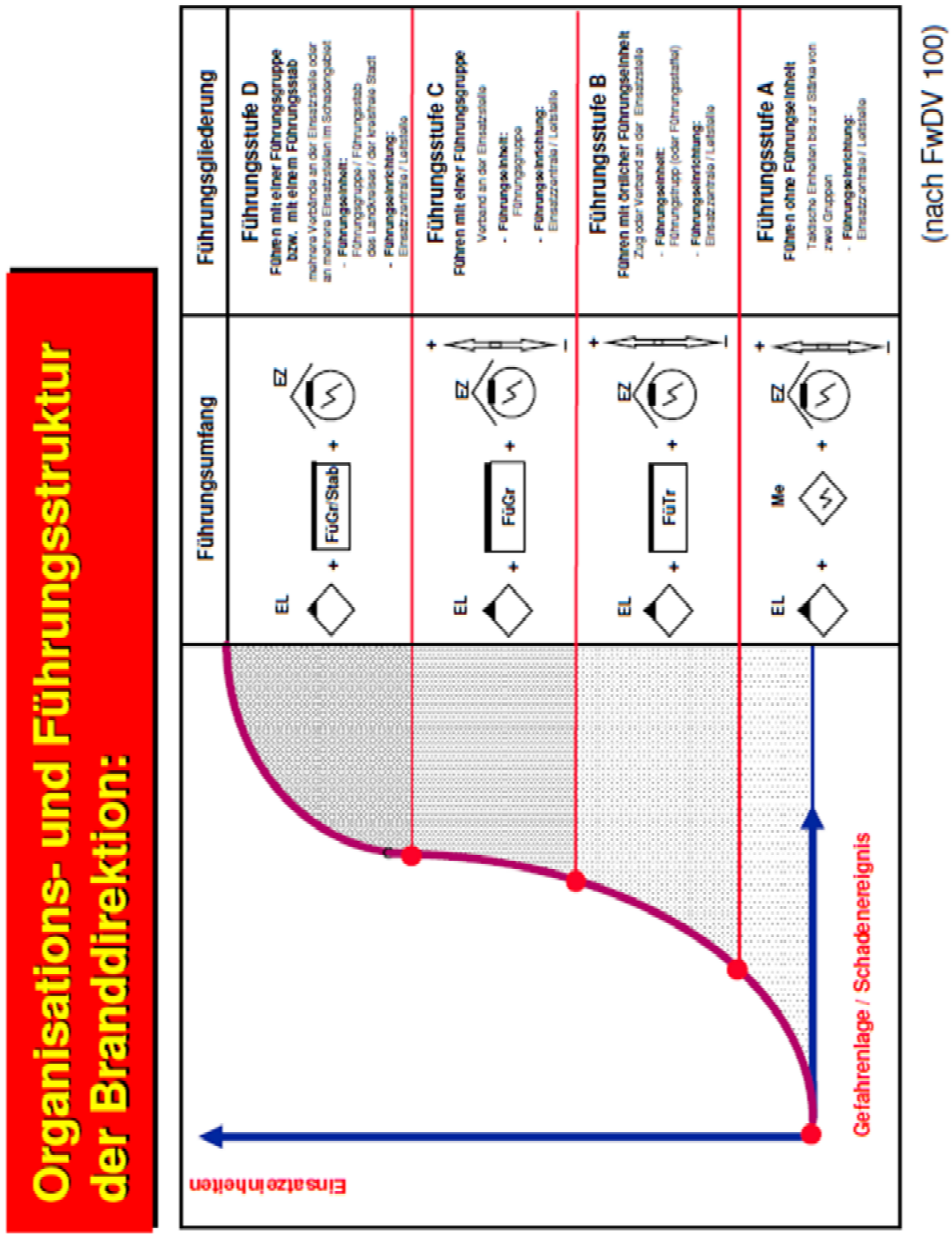
Lagemeldungen:

- Die Zentralen der Unternehmen des Lebensmittelhandels, sowie Träger von ambulante Pflegedienstendes und soziale Einrichtungen fordern die bevorzugte Verteilung von antiviralen Medikamenten an ihr Personal, da dieses einem erhöhten Infektionsrisiko ausgesetzt sind.
- Bei einem starken Unwetter über den östlichen Stadtteilen Stuttgarts, kam es zu einer Vielzahl von Einsatzstellen die von den verfügbaren Kräften der Berufs- und Freiwilligen Feuerwehr abgearbeitet wurden, hierbei unterstütze das THW mit Spezialkräften und –gerät.
- Erhöhte Inanspruchnahme der Seelsorger und psychologischen Beratungsstellen durch Angehörige von Grippeopfern, als Folge aktiviert das Sozialamt das GSE-Modul 31 „Sicherstellung der psychosozialen Notfallversorgung bei Großschadensereignissen in der [redacted]
- Das Garten-, Friedhofs- und Forstamt teilt mit, dass das Fachpersonal aufgrund der Vielzahl von Toten physisch und psychisch erschöpft sei.
- Infolge des Ausfalls der zentralen Telefonnummer [redacted] der Stadt und der anschließenden Weiterleitung auf das Bürgertelefon kommt es hier zu Wartezeiten für die Anrufer.
- Einer von 3 Öfen des Krematoriums auf dem Pragfriedhof ist dauerhaft ausgefallen, da die Schamottverkleidung eingestürzt ist.
- Am [redacted] gibt es Panikreaktionen von Fahrgästen aufgrund der Interaktion von hysterischen Personen. Die Hysterien wurden offenbar durch heftige Hustenanfälle von Passanten (in einem Einzelfall Husten mit blutigem Auswurf) ausgelöst.
- [redacted] meldet, dass erkranktes Personal ersetzt werden muss. Ein Weiterbetrieb mit noch weniger Mitarbeitern ist nicht möglich, hierdurch werden auch die Instandsetzungs- und Wartungsarbeiten am Strom- und Wassernetz verzögert. Die [redacted] hält abgepacktes Trinkwasser (Schlauchpackung 1 l Inhalt) vor, kann dies jedoch aus Mangel an Mitarbeitern nicht zur Einsatzstelle transportieren.
- Die Landwirtschaftskammer teilt mit, dass die Landwirte eine erhebliche Verknappung an Futtermitteln, insbesondere für die Schlachtvieherzeugung, verzeichnen. Es gibt Probleme, die Fütterung in dem erforderlichen Umfang aufrecht zu erhalten. Teilweise können Lieferanten ihren Lieferverpflichtungen nicht mehr nachkommen. Erhöhte Preise versetzen darüber hinaus die Landwirte in eine schwierige Lage.
- Die Rettungsdienste melden steigende Einsatzzahlen. Dies erfordert in der Integrierten Rettungsleitstelle eine angepasste Logistik. Personalausfälle müssen kompensiert und die Anzahl der Leitstellendisponenten dem Einsatzaufkommen angepasst werden.
- Dauerüberweisungen, Lastschriften (Miete, Strom, Kredittilgungen) auf Privat- und Geschäftskonten werden nur noch eingeschränkt verarbeitet da die Quelldaten nicht verfügbar sind.
- Der Krankenstand des Hochbauamtes beträgt ca. 60 % der Mitarbeiter, darüber hinaus können weitere Fachämter nur noch einen Notbetrieb aufrechterhalten.


Der Verwaltungsstabes (VwS)
in den Alarmstufen „orange“ und „rot“
Führungs- und Lage-
zentrum der Polizei
Integrierte Leitstelle
(ILS)
Alarmstufen
„orange / rot“
THW
RD
BW
Einsatzleitung
(vor Ort)
VwS
FüS
LdS *
10
37
53
L/OB
+ -K
32
36
PVD
Stabsgruppe
zusätzlich:
- Ämter
- sonstige
Orga-Einheiten
- Eigenbetriebe
und
- Fachberater
VwS
BPol
Bundespolizei
...
...


Organisation in
[redacted]
[redacted]
IVLZ
VwS
ILS
FüS
AföO
Tiefbauamt
[redacted]
Polizei
Feuerwehr
DRK
[redacted]


Der Führungsstab (FüS) und Verwaltungsstab (VwS)
Organigramm des Verwaltungs- und Führungsstabes
Behördenleiter
- Oberbürgermeister -
administrativ-organisatorisch
Verwaltungsstab (VwS)
mit Leitung des Stabes (LdS)
Stabsgruppe (SMS)
VwS-KGS*
Information
operativ-taktisch
Technische Einsatzleitung
Führungsstab (FüS)
mit Leitung des Stabes (LdS)
S 1
S 2
S 3
S 4
S 5
S 6
Zusätzlich über das Sachgebiet 3 organisatorisch angegliedert sind
Ämter
Ämter
Eigenbetriebe
...
In Kontakt mit
Integrierte Leitstelle Stuttgart
Führungs- und Lagezentrum (FLZ) der Polizei
Abschnittsleitung vor Ort
Abschnittsleitung vor Ort
Abschnittsleitung vor Ort
...

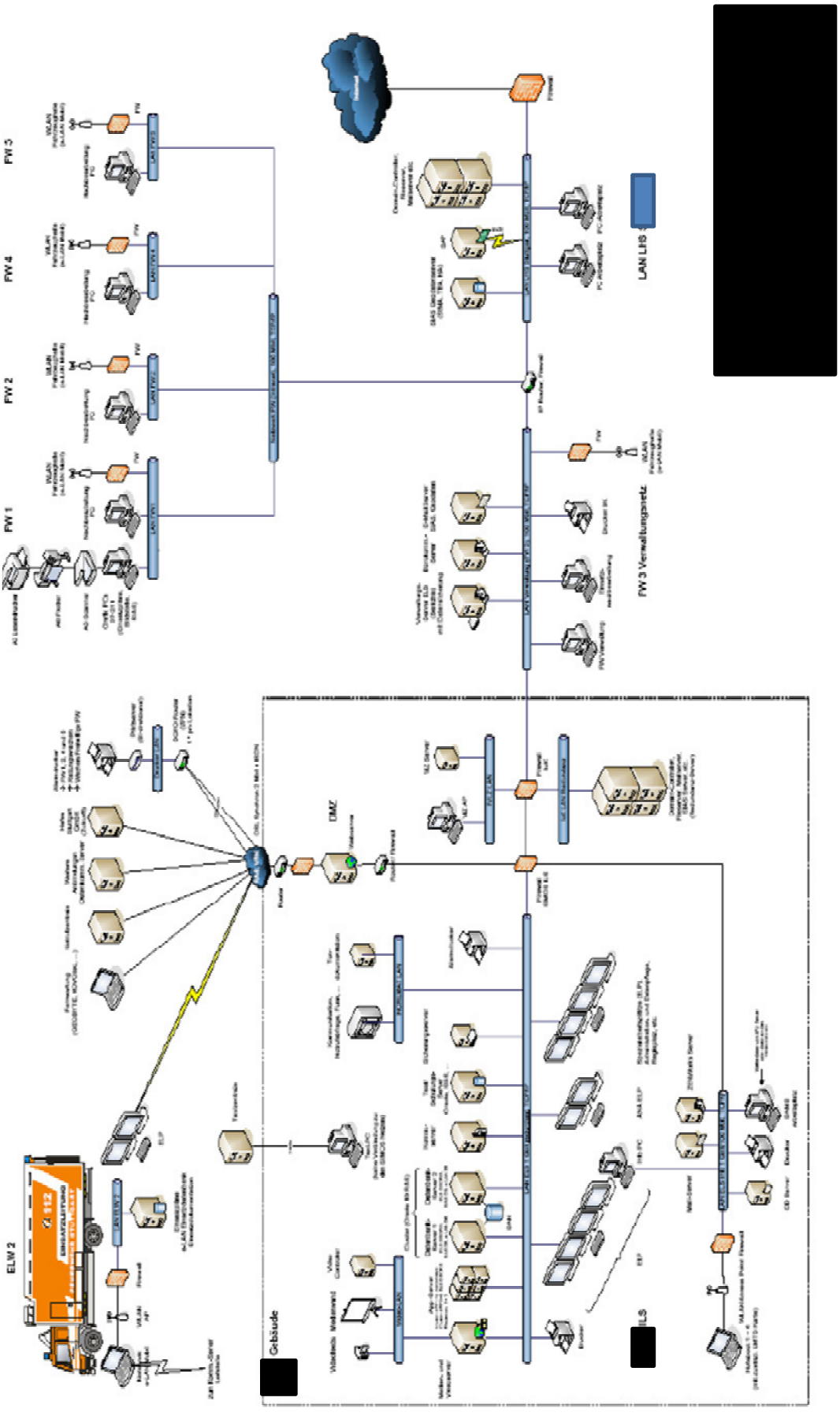

Organisations- und Führungsstruktur der Branddirektion:
Führungsgliederung
Führungsumfang
Führungsstufe D
Führen mit einer Führungsgruppe bzw. mit einem Führungsstab
Führungsstufe C
Führen mit einer Führungsgruppe
Führungsstufe B
Führen mit örtlicher Führungseinheit
Führungsstufe A
Führen ohne Führungseinheit
EL
EZ
FüGr/Stab
FüGr
FüTr
Me
Einsatzeinheiten
Gefahrenlage / Schadenereignis
(nach FwDV 100)

Die Alarmstufen:
Verwaltungsstab
als Präsenzstab
Stabsgruppe (SGr)
als Kernbereich des
Verwaltungsstabes
amtsinterne
Führungsstrukturen
Alarmstufen
Situation
„rot“
„orange“
„gelb“
VwS
im Sinne eines
Katastrophen-
schutzstabes
VwS
VwS-SGr
Tägliche Gefahrenabwehr
„Normalzustand“
„außergewöhnliches Ereignis“
* = abhängig von Ämtern und Szenarien

Alarmstufen „gelb“ bis „rot“: Großschadenslage

Alarmstufen	operativ-taktisch* vor Ort	operativ-taktisch* rückwärtig	administrativ-organisatorisch
Katastrophe	Je nach Lage einer Katastrophe (punktuelles oder flächiges Ereignis) werden **Abschnittsleitungen** gebildet	**Technische Einsatzleitung** im Stabsraum in [redacted] Technischer Einsatzleiter: Bestellung, ansonsten Amtsleiter 37	**Verwaltungsstab (VwS)** als Katastrophenschutzstab Leitung: Bestellung Von der Behördenleitung beauftragter Bürgermeister
außergewöhnliches Ereignis	**Abschnittsleitungen** Abschnittsleiter: Leitungsebene der zuständigen Organisationseinheit	**Einsatzleitung** Einsatzleiter: Leitungsebene der zuständigen Organisationseinheit	**Verwaltungsstab (VwS)** Leitung: Bestellung Von der Behördenleitung beauftragter Bürgermeister
	Abschnittsleitungen Abschnittsleiter: Leitungsebene der zuständigen Organisationseinheit	**Einsatzleitung** Einsatzleiter: Leitungsebene der zuständigen Organisationseinheit	**Stabsgruppe (VwS-SGr)** als Kernbereich des Verwaltungsstabes (VwS) Leitung: **lageabhängig** Leiter der zuständigen Organisationseinheit oder Beauftragter des Behördenleiters.

* Einheiten der Feuerwehr und des Katastrophenschutzes


FW 5
FW 4
FW 2
FW 1
LAN LFS
FW 3 Verwaltungsnetz
DMZ
ELW 2
Gebäude
LS

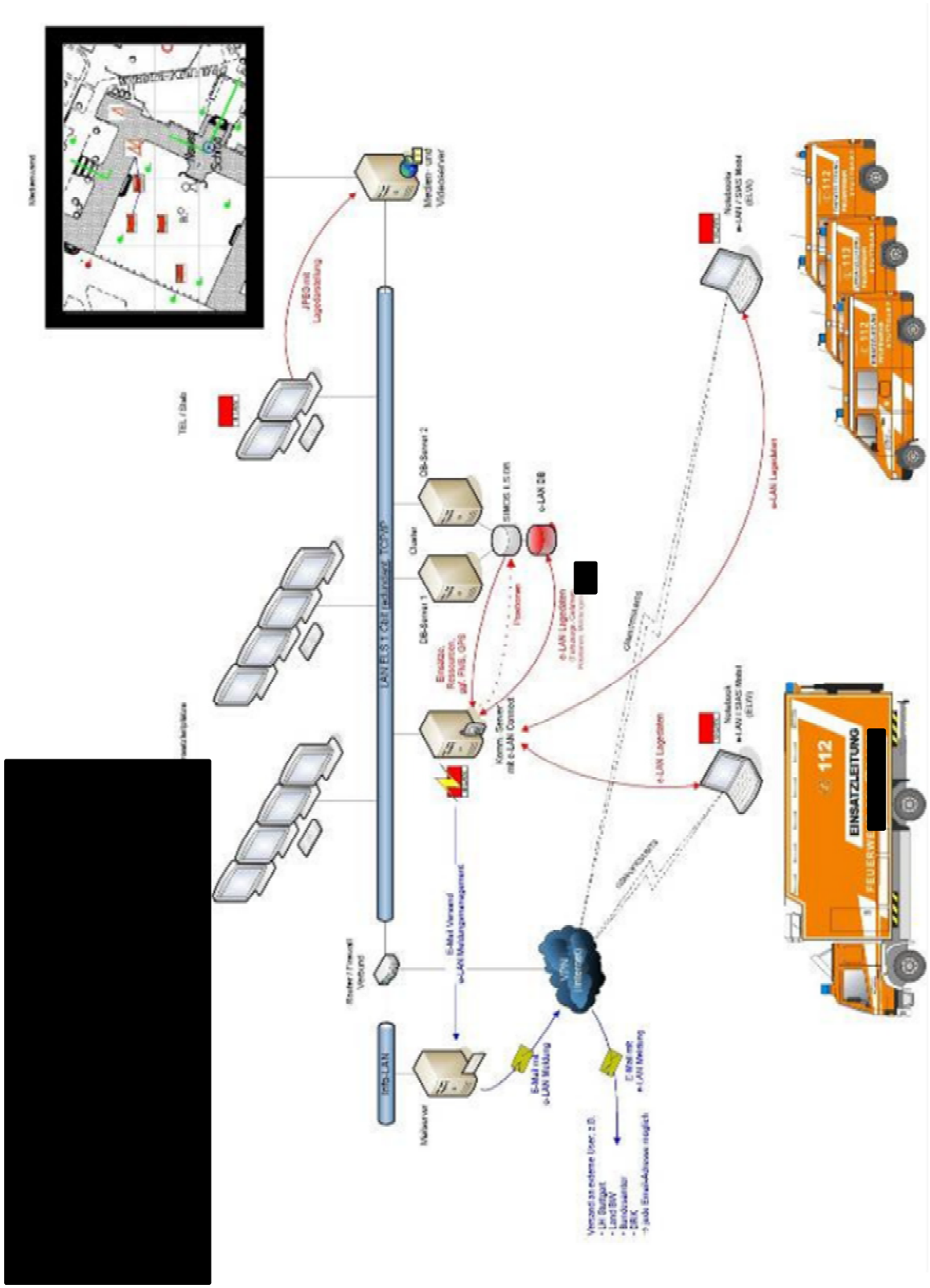
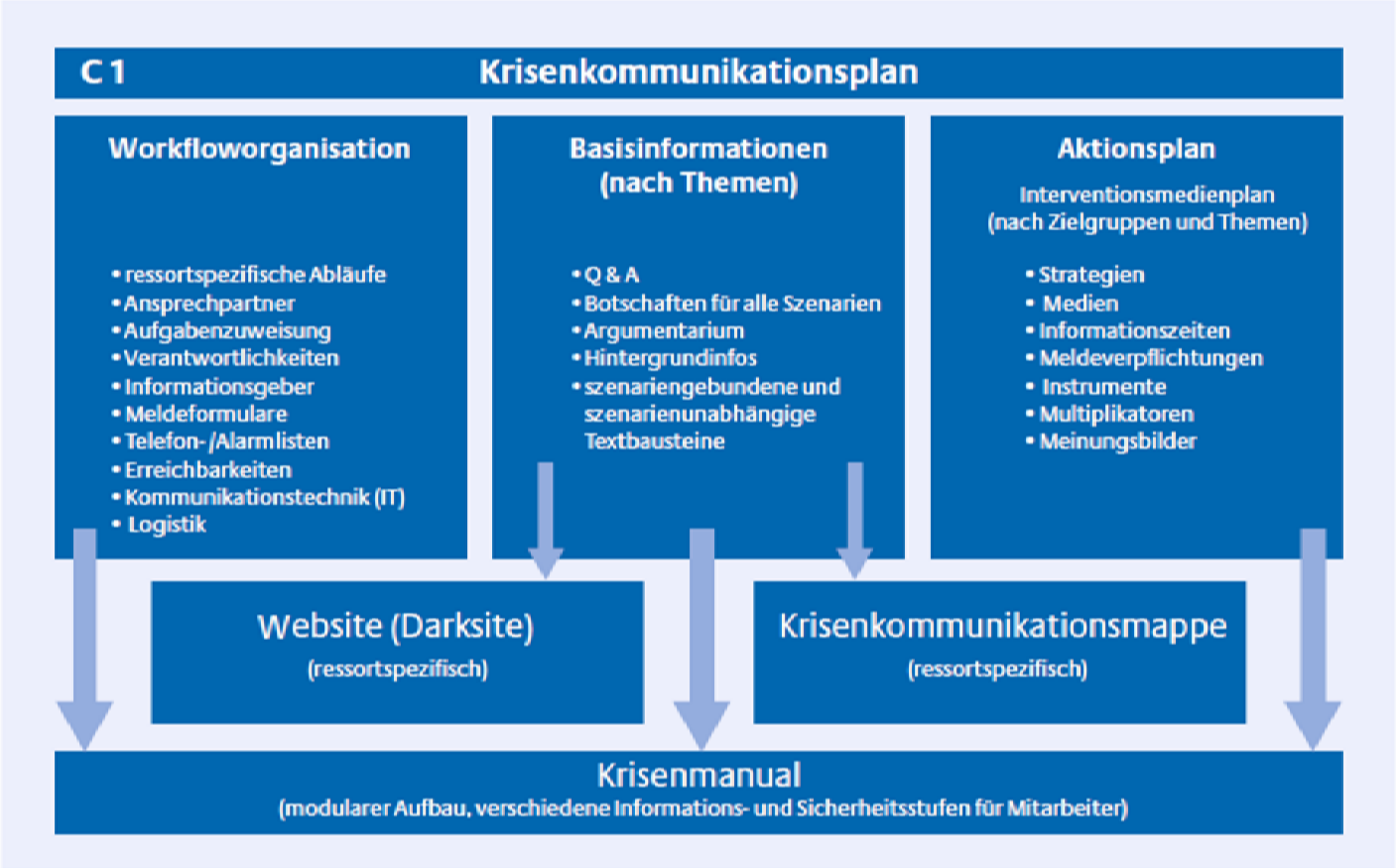

LAN FEST GBT technical TOPO
Medien- und Videoserver
DB-Server 2
Cluster
DB-Server 1
SIMOS 8.5 ION
e-LAN DB
Komm. Server mit e-LAN Connect
Router / Firewall Verbund
Info-LAN
Mailserver
VPN (Internet)
Notebook e-LAN / SIAS Modul (BLW)
e-LAN Logistiken
Übertragung
E-Mail Versand e-LAN Meldungsmanagement
E-Mail mit e-LAN Meldung
112
EINSATZLEITUNG
FEUERWEHR

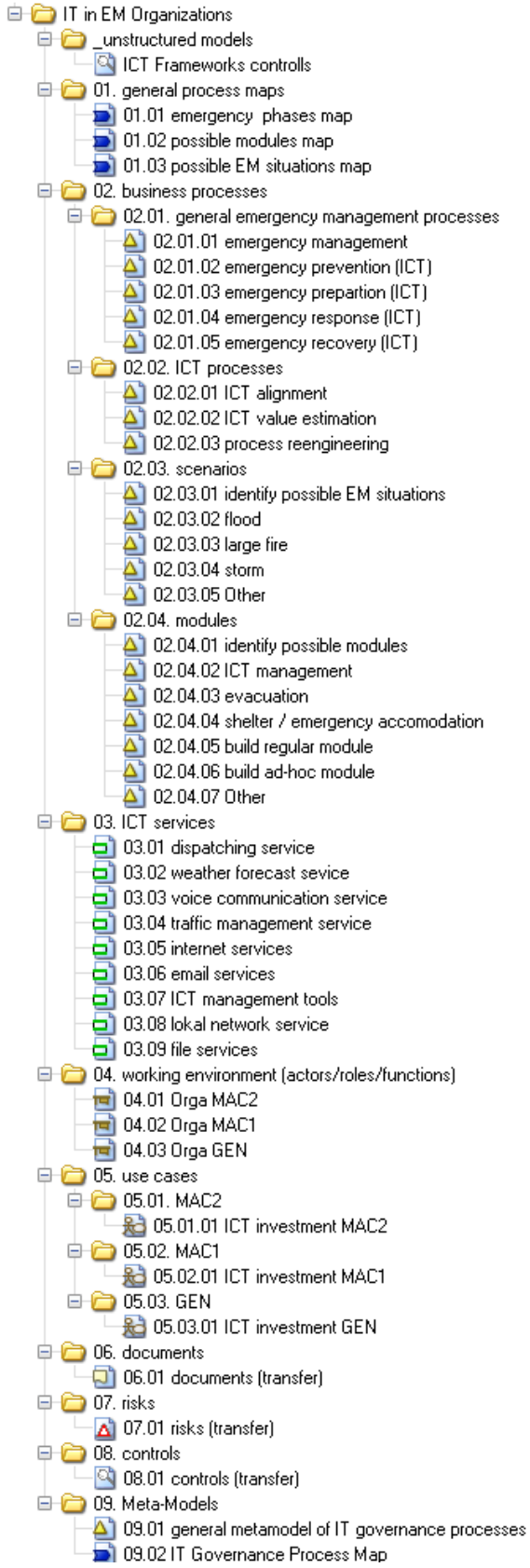
Abbildung 4: Krisenkommunikationsplan[27]

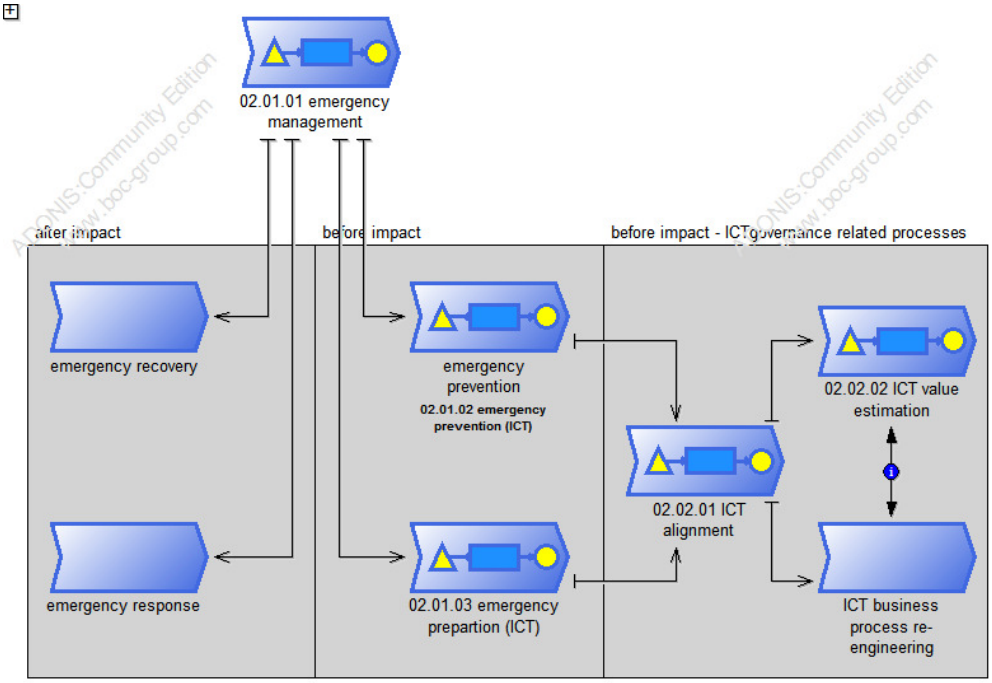


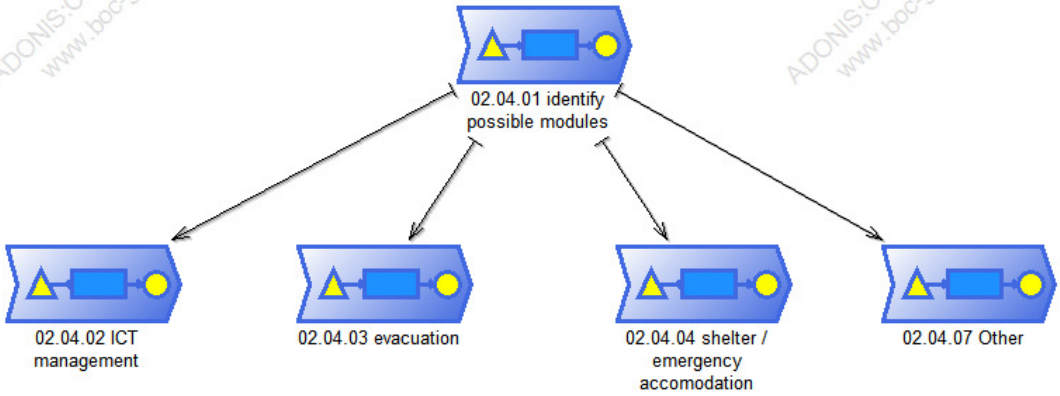
[26] Gilt für vorhersehbare Krisen beziehungsweise den abstrakten Ablauf der Krisenkommunikation.

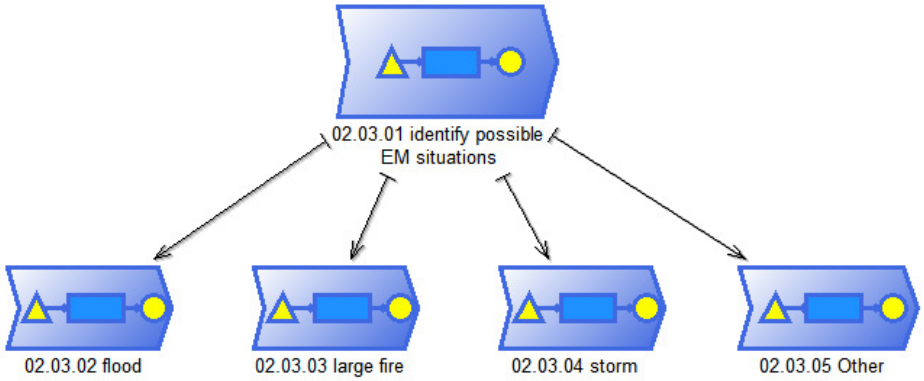
[27] Vgl. Sorina Hamburger: Möglichkeiten und Grenzen der Krisenkommunikation (Studienarbeit vom 11. Januar 2006), a. a. O., Seite 10 (vom Autor verändert).

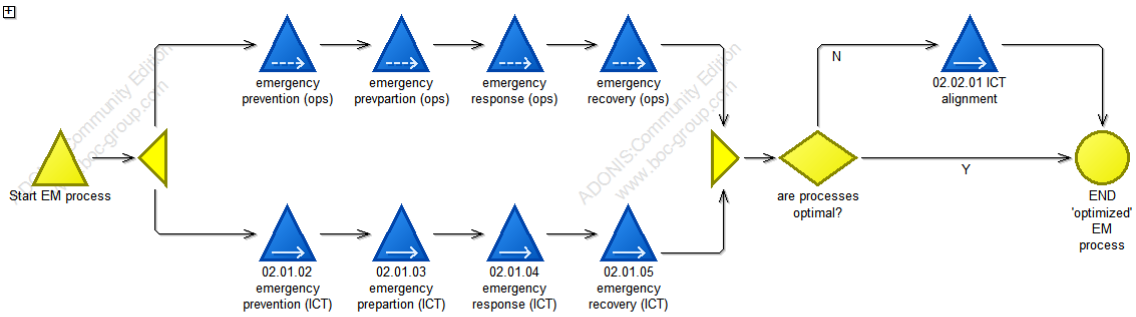
16 Appendix D (Model & Process Documentation)

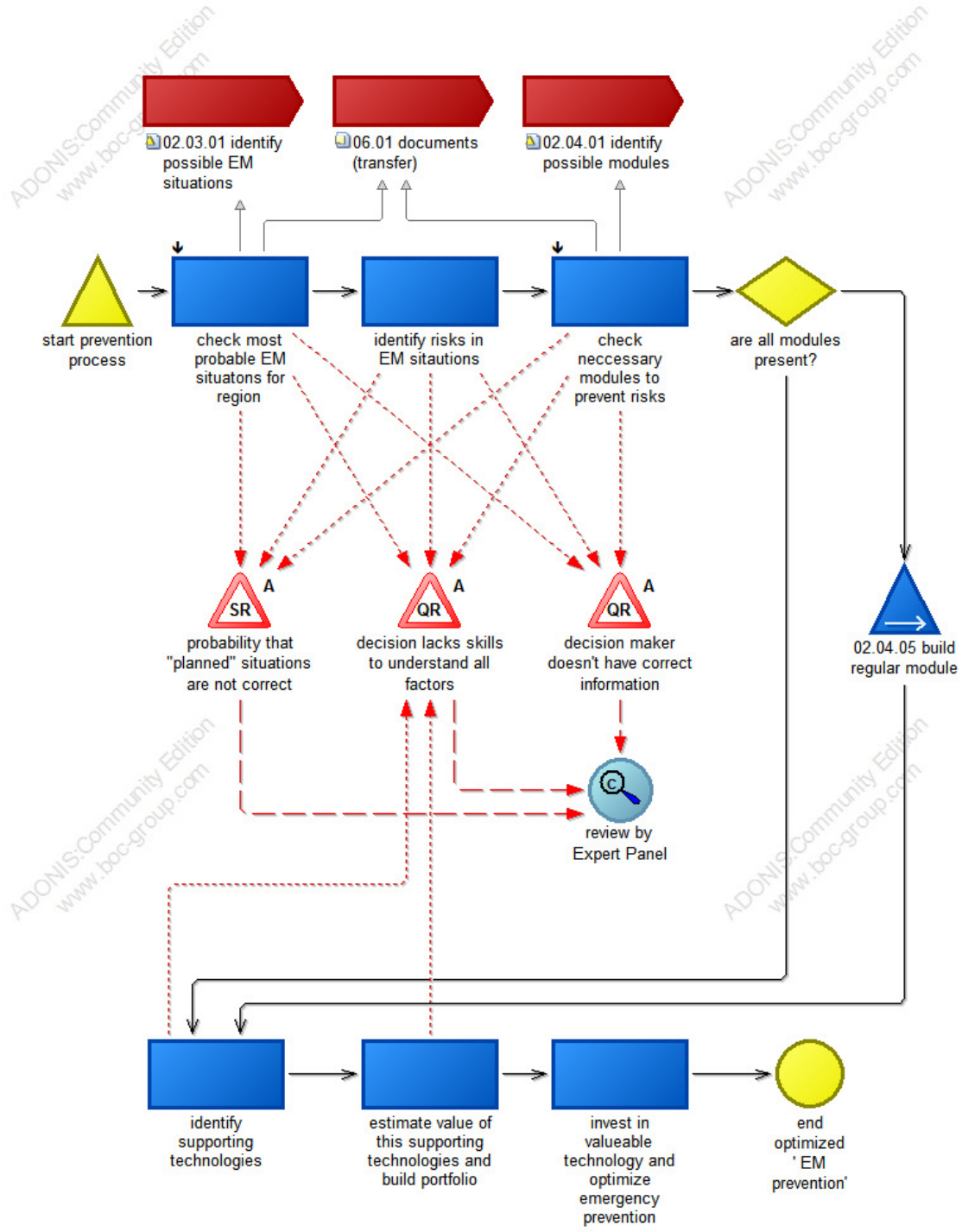


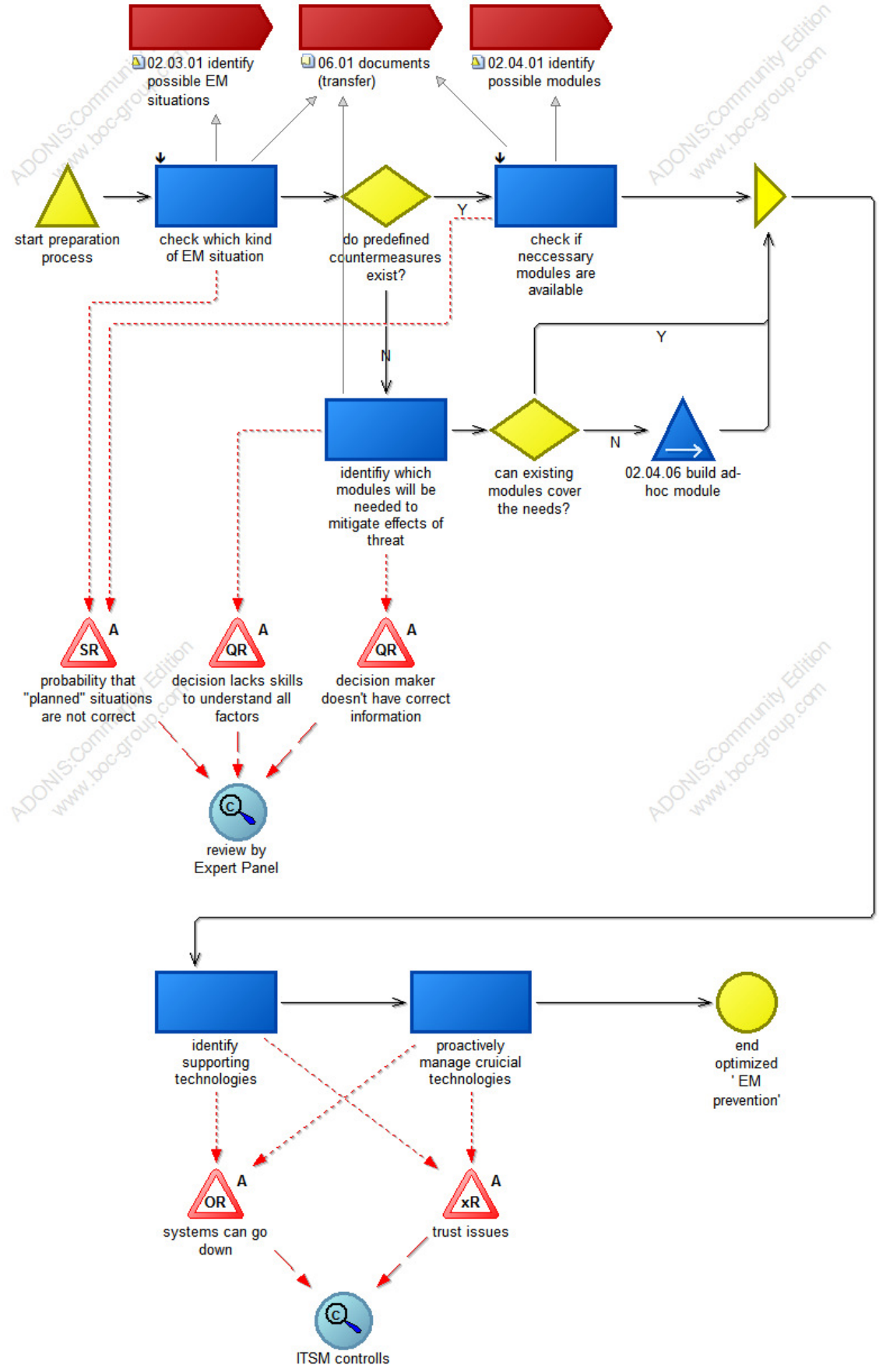


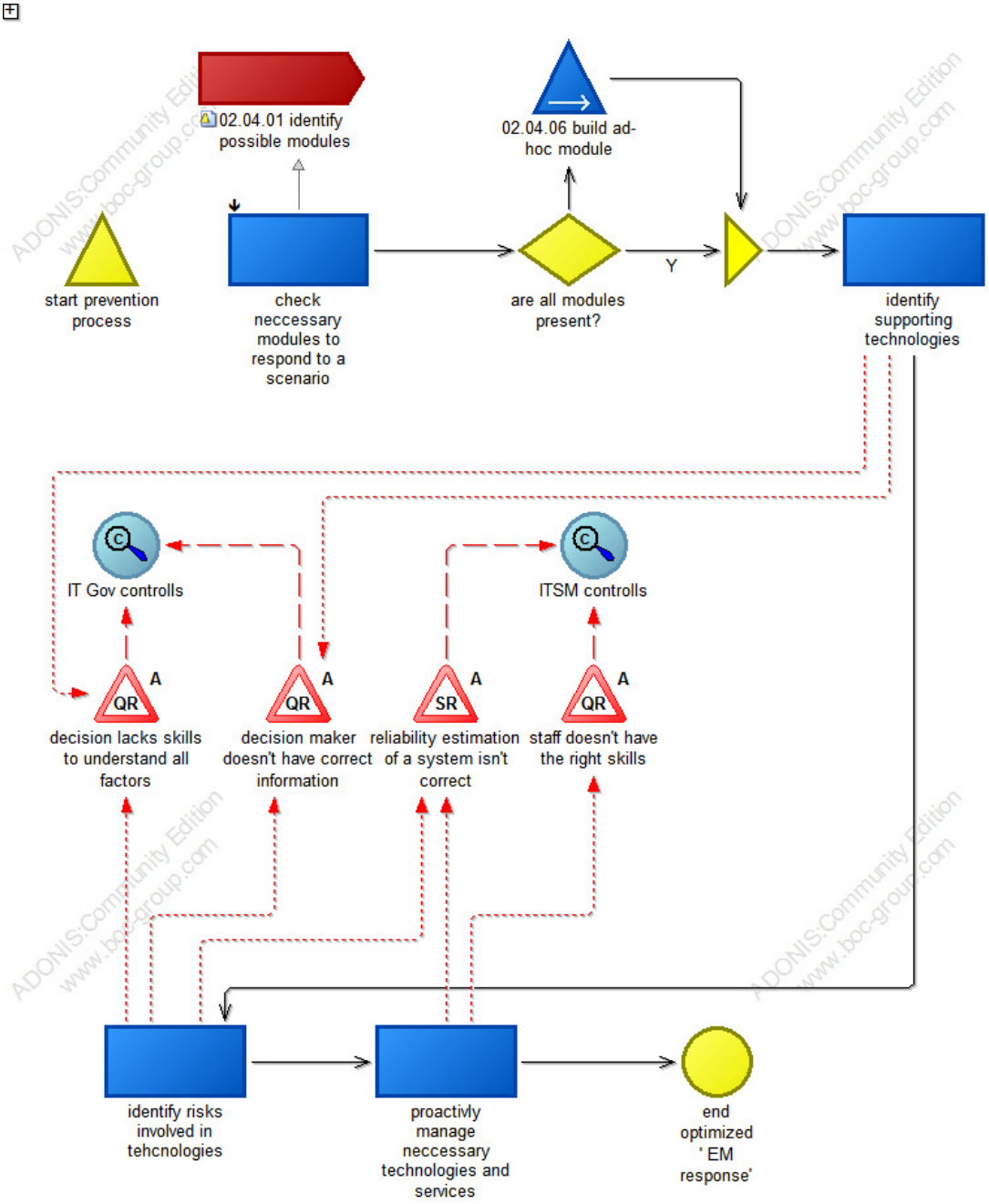


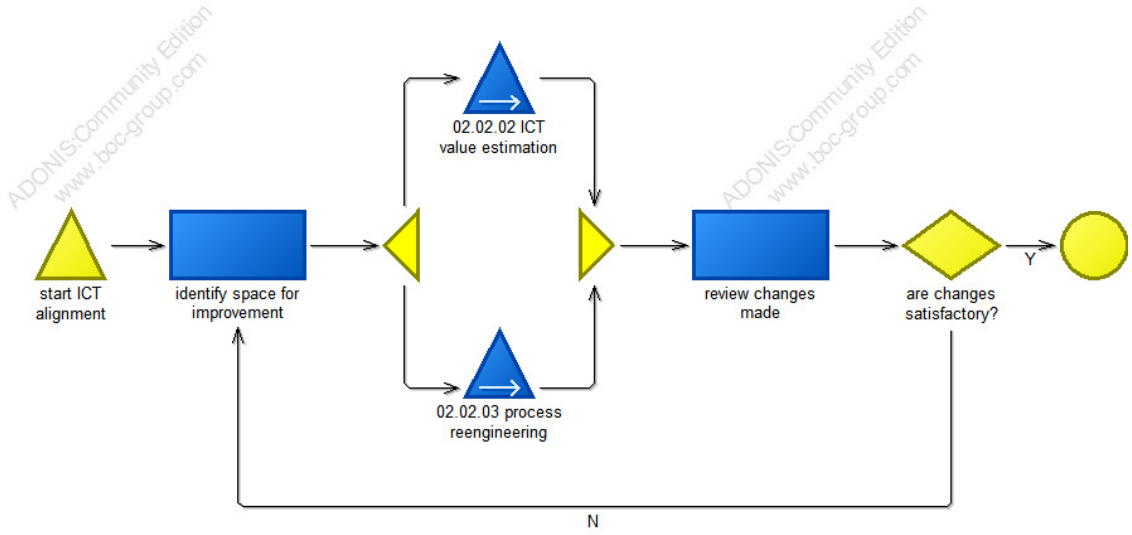


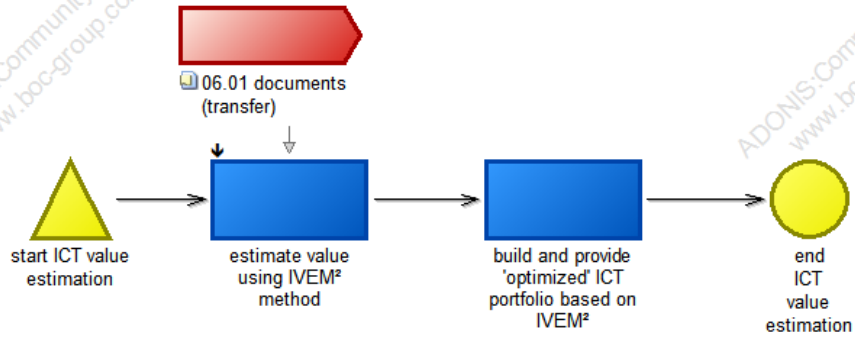


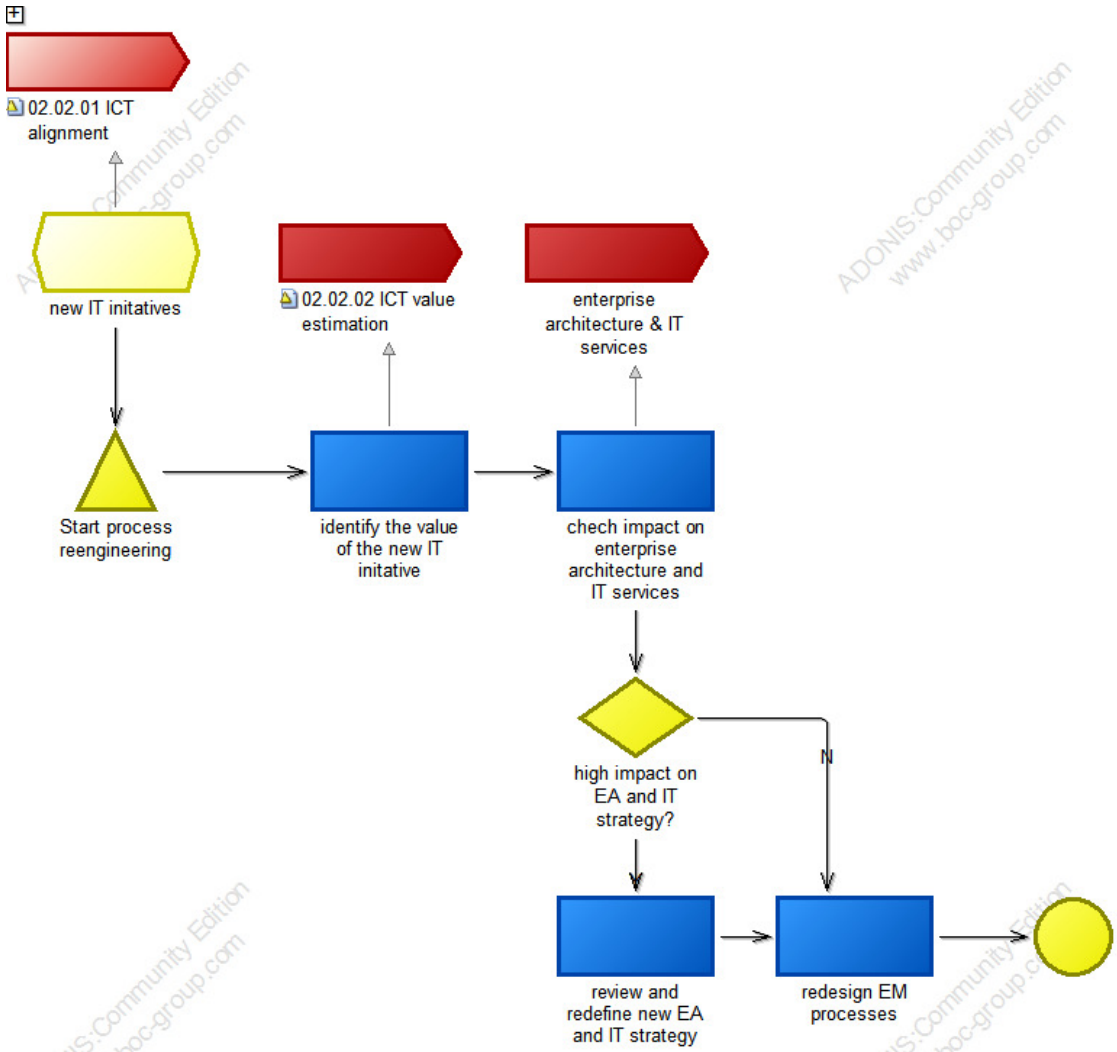

02.03.01 identify possible EM situations
06.01 documents (transfer)
02.04.01 identify possible modules
start prevention process
check most probable EM situatons for region
identify risks in EM sitautions
check neccessary modules to prevent risks
are all modules present?
A
SR
probability that "planned" situations are not correct
A
QR
decision lacks skills to understand all factors
A
QR
decision maker doesn't have correct information
02.04.05 build regular module
review by Expert Panel
identify supporting technologies
estimate value of this supporting technologies and build portfolio
invest in valueable technology and optimize emergency prevention
end optimized ' EM prevention'

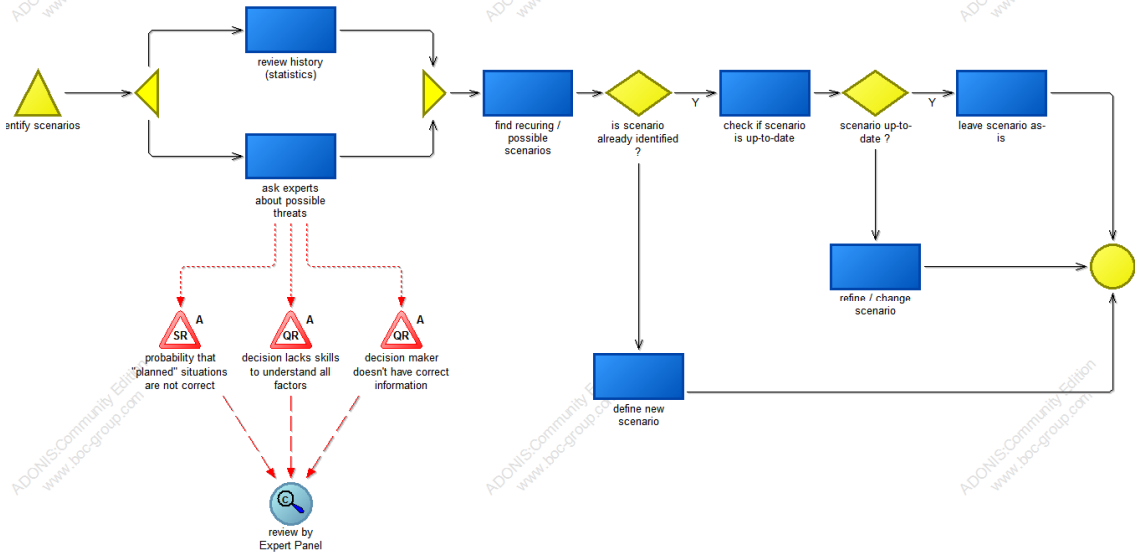

02.03.01 identify possible EM situations
06.01 documents (transfer)
02.04.01 identify possible modules
start preparation process
check which kind of EM situation
do predefined countermeasures exist?
check if neccessary modules are available
Y
N
Y
identify which modules will be needed to mitigate effects of threat
can existing modules cover the needs?
N
02.04.06 build ad-hoc module
A
SR
probability that "planned" situations are not correct
A
QR
decision lacks skills to understand all factors
A
QR
decision maker doesn't have correct information
review by Expert Panel
identify supporting technologies
proactively manage cruicial technologies
end optimized ' EM prevention'
A
OR
systems can go down
A
xR
trust issues
ITSM controlls
ADONIS:Community Edition
www.boc-group.com

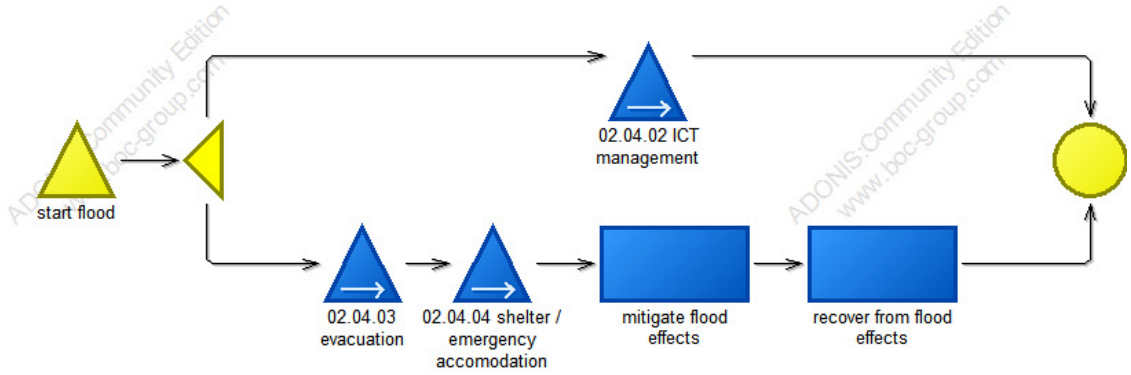

02.04.01 identify possible modules
02.04.06 build ad-hoc module
start prevention process
check neccessary modules to respond to a scenario
are all modules present?
Y
identify supporting technologies
IT Gov controlls
ITSM controlls
A
QR
decision lacks skills to understand all factors
A
QR
decision maker doesn't have correct information
A
SR
reliability estimation of a system isn't correct
A
QR
staff doesn't have the right skills
identify risks involved in tehcnologies
proactivly manage neccessary technologies and services
end optimized ' EM response'

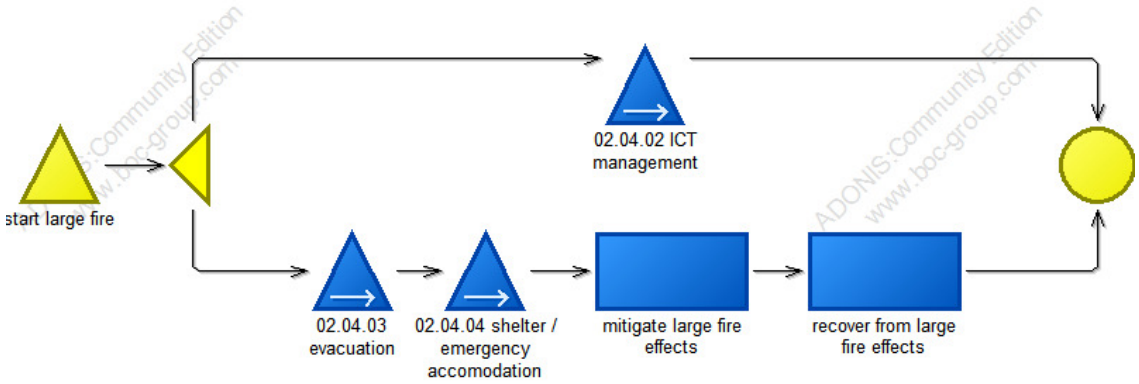


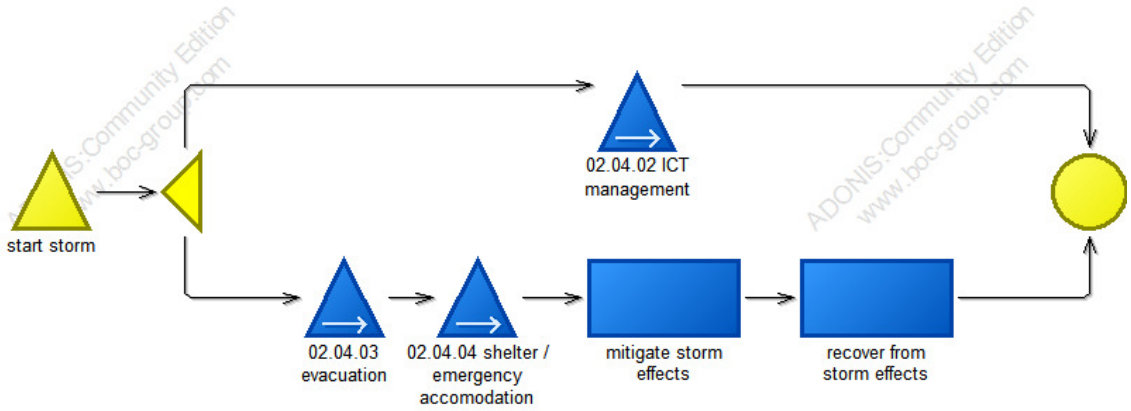


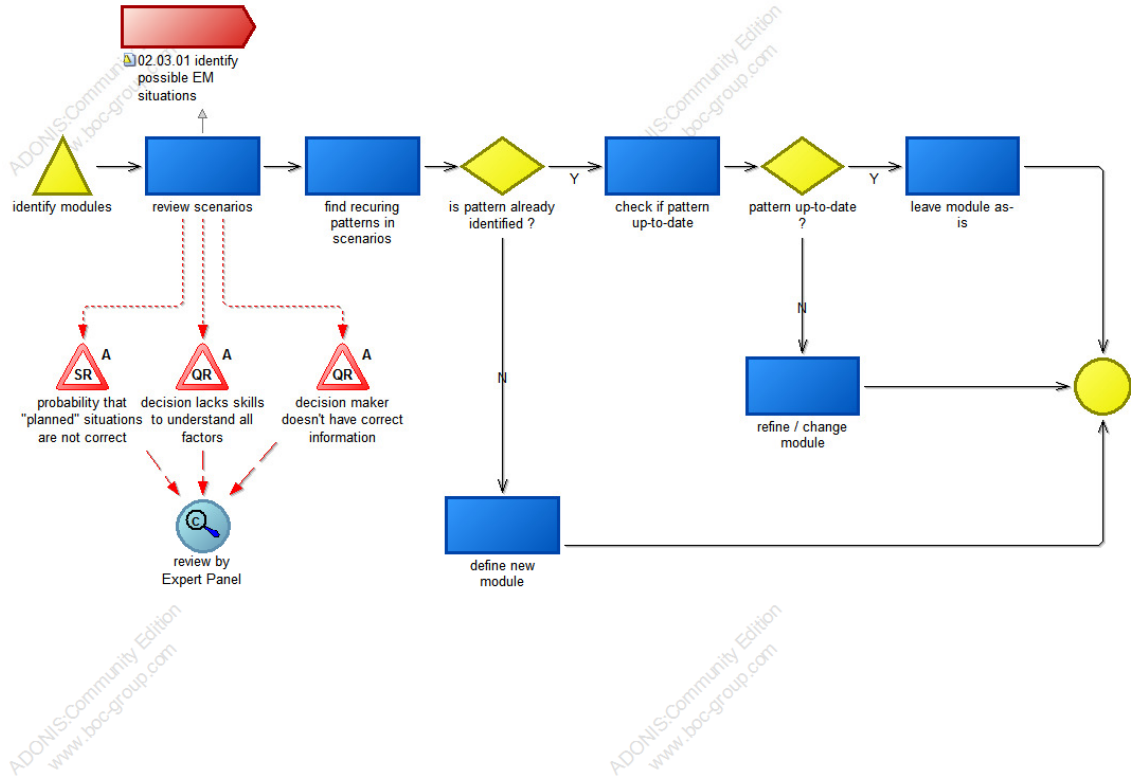

02.02.01 ICT alignment
new IT initatives
02.02.02 ICT value estimation
enterprise architecture & IT services
Start process reengineering
identify the value of the new IT initative
chech impact on enterprise architecture and IT services
high impact on EA and IT strategy?
N
review and redefine new EA and IT strategy
redesign EM processes
ADONIS:Community Edition
www.boc-group.com

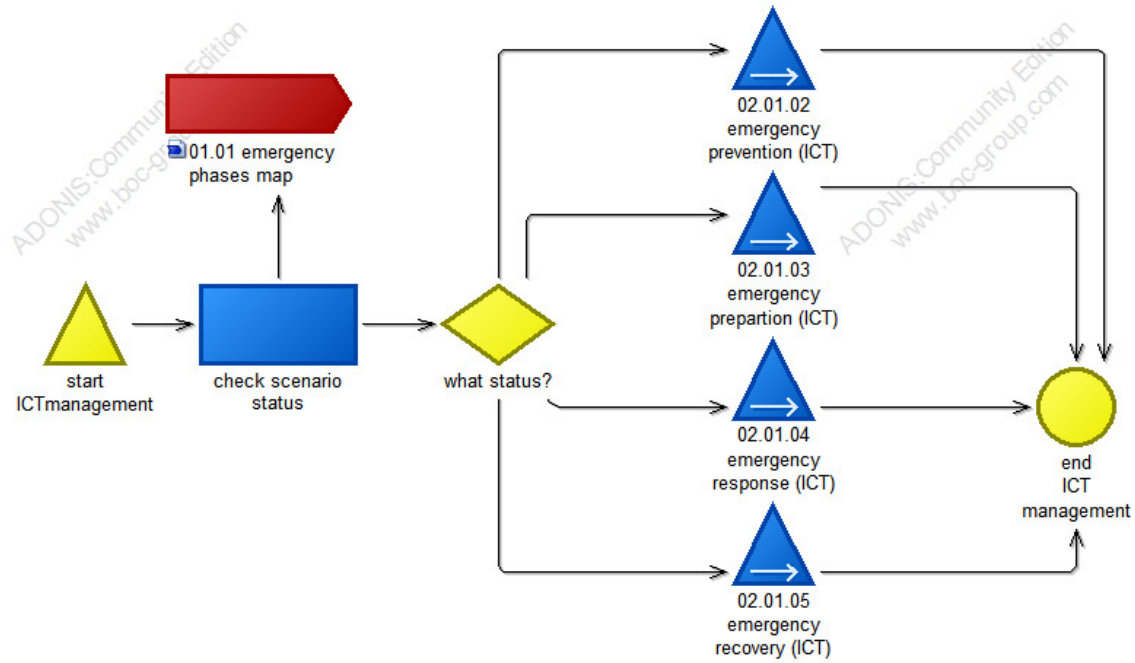

review history (statistics)
ntify scenarios
ask experts about possible threats
find recuring / possible scenarios
is scenario already identified ?
Y
check if scenario is up-to-date
scenario up-to-date ?
Y
leave scenario as-is
refine / change scenario
define new scenario
SR
A
probability that "planned" situations are not correct
QR
A
decision lacks skills to understand all factors
QR
A
decision maker doesn't have correct information
review by Expert Panel

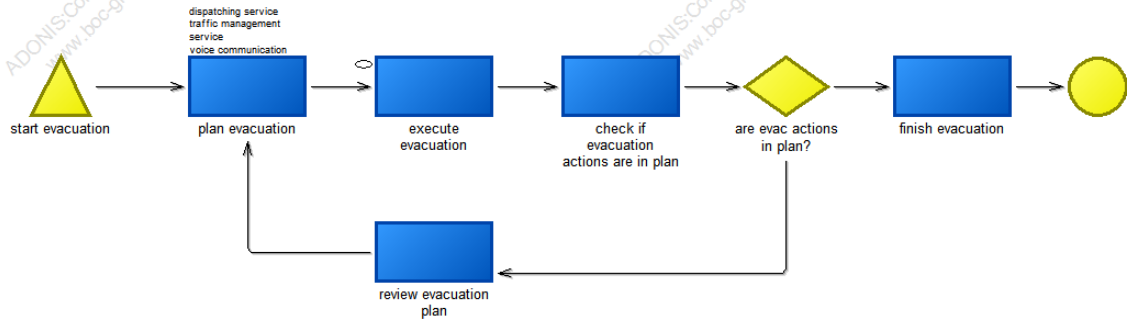


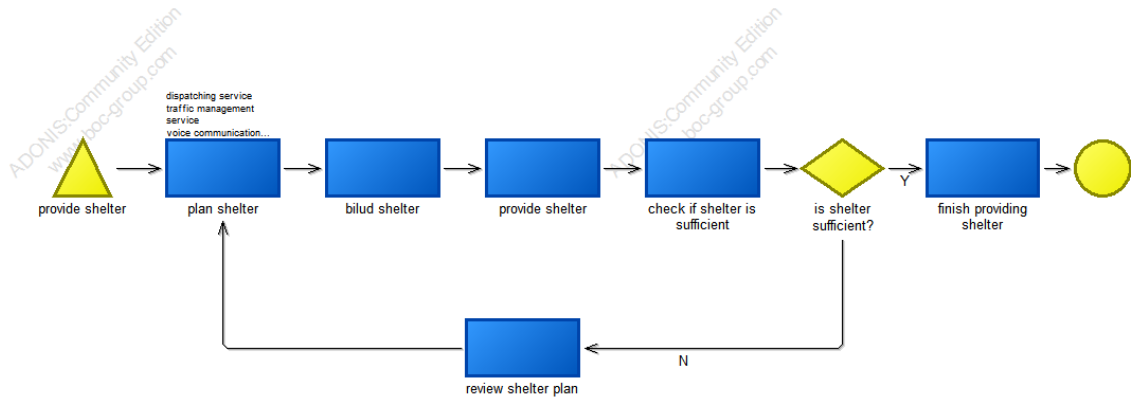


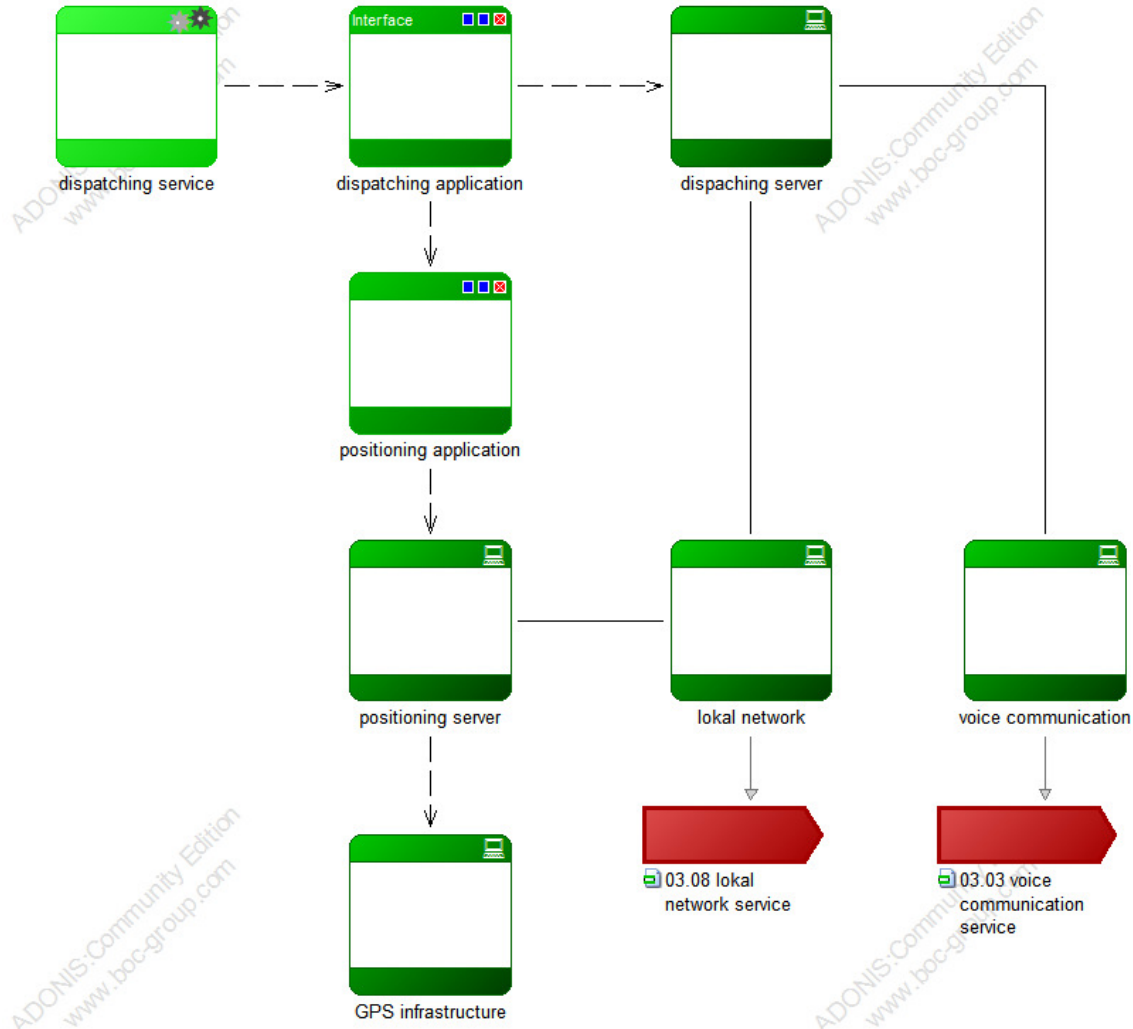


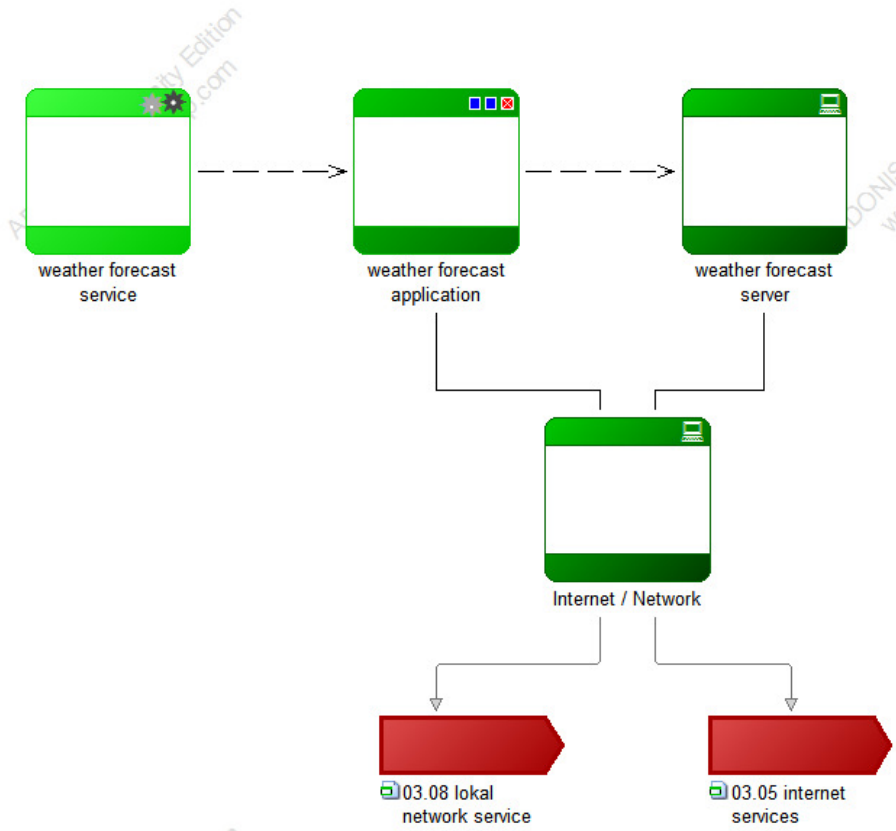

02.03.01 identify possible EM situations
identify modules
review scenarios
find recuring patterns in scenarios
is pattern already identified ?
Y
check if pattern up-to-date
pattern up-to-date ?
Y
leave module as-is
N
refine / change module
N
define new module
A
SR
probability that "planned" situations are not correct
A
QR
decision lacks skills to understand all factors
A
QR
decision maker doesn't have correct information
review by Expert Panel
ADONIS:Community Edition
www.boc-group.com

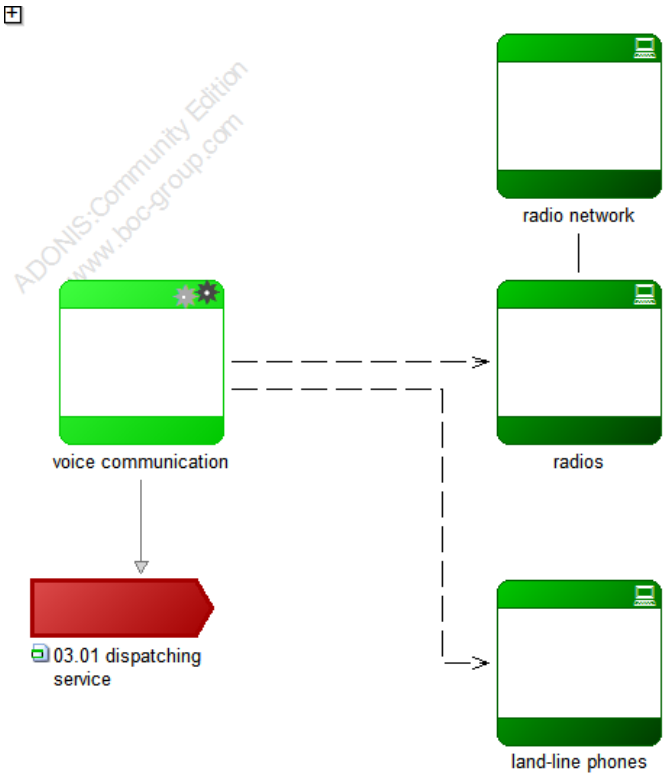


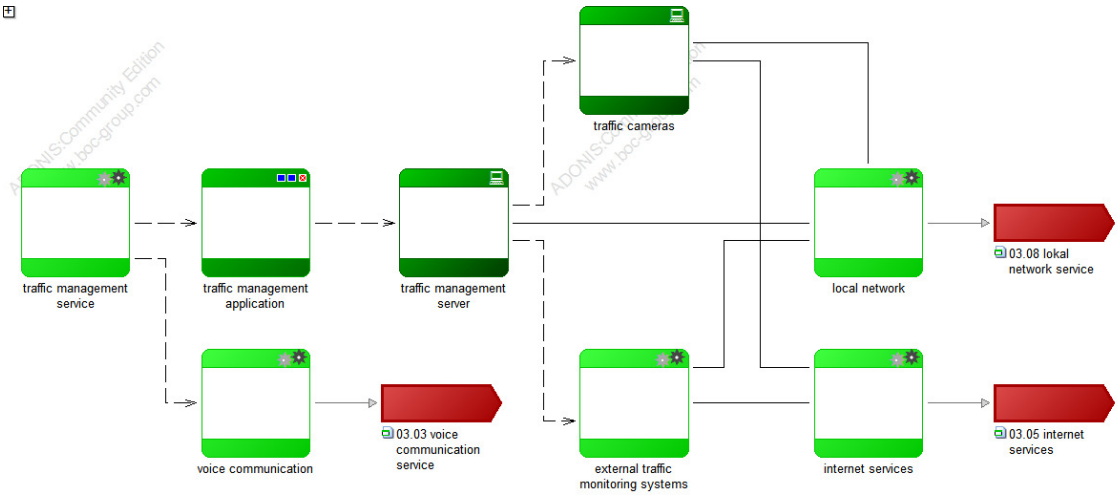


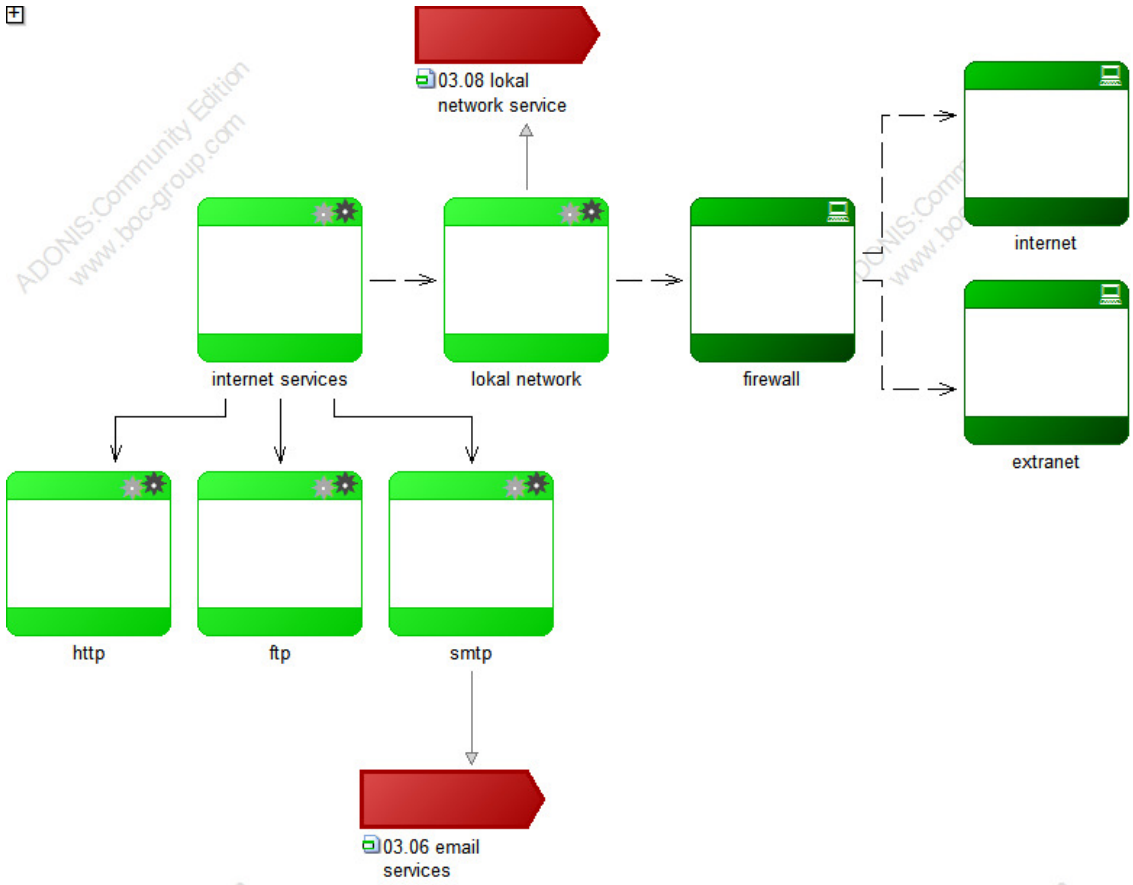


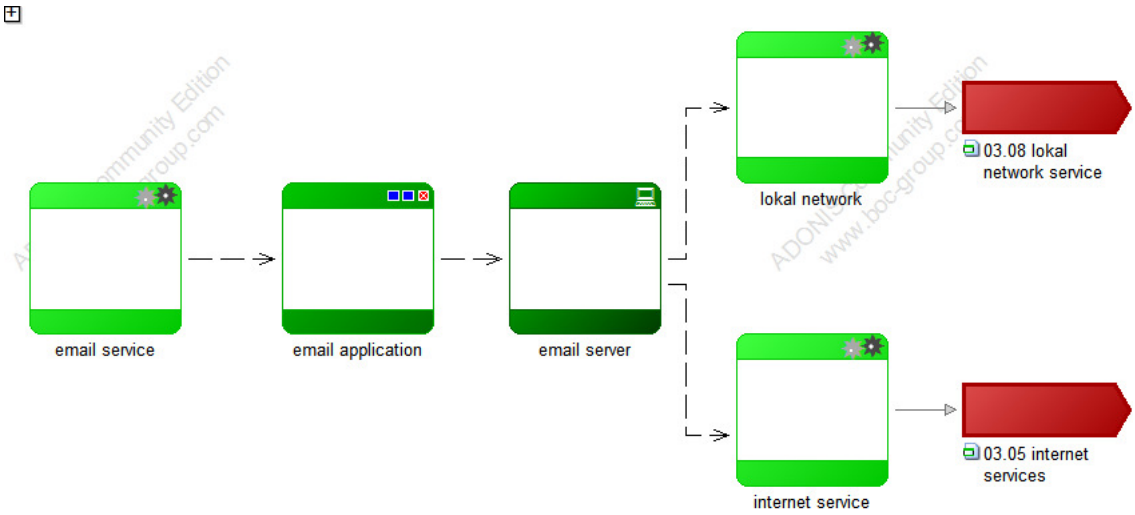

dispatching service
Interface
dispatching application
dispaching server
positioning application
positioning server
lokal network
voice communication
03.08 lokal network service
03.03 voice communication service
GPS infrastructure

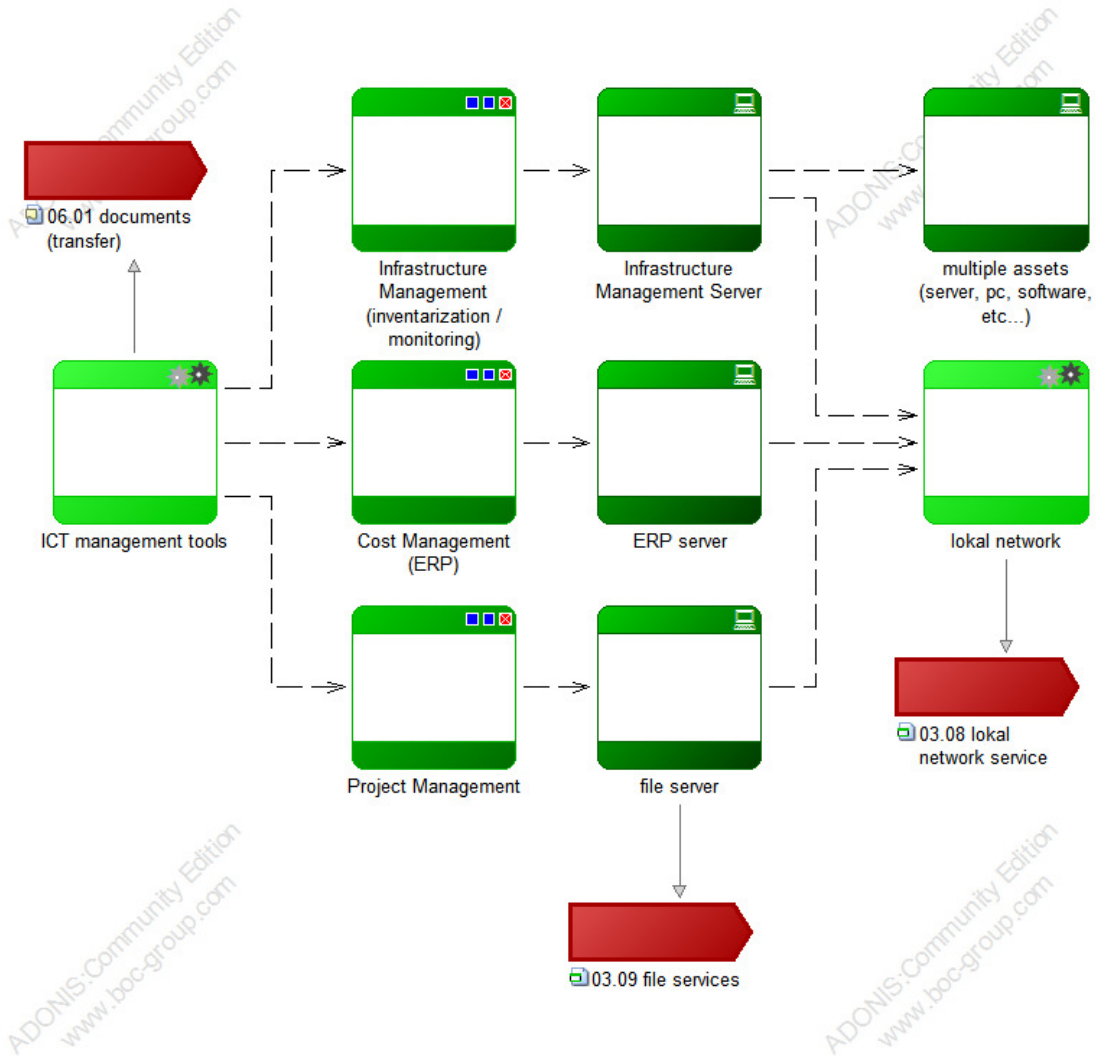


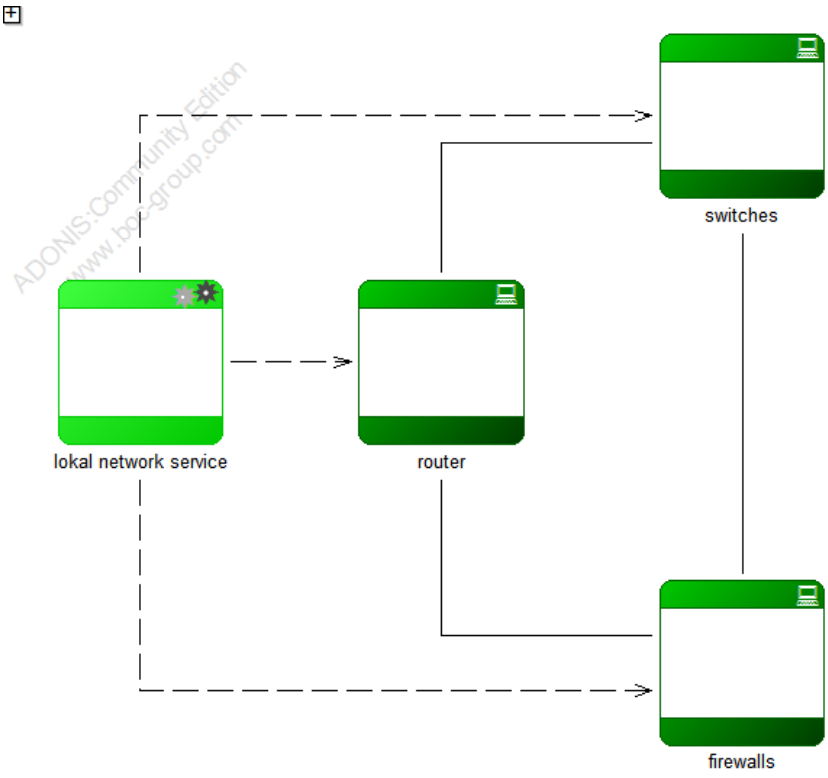


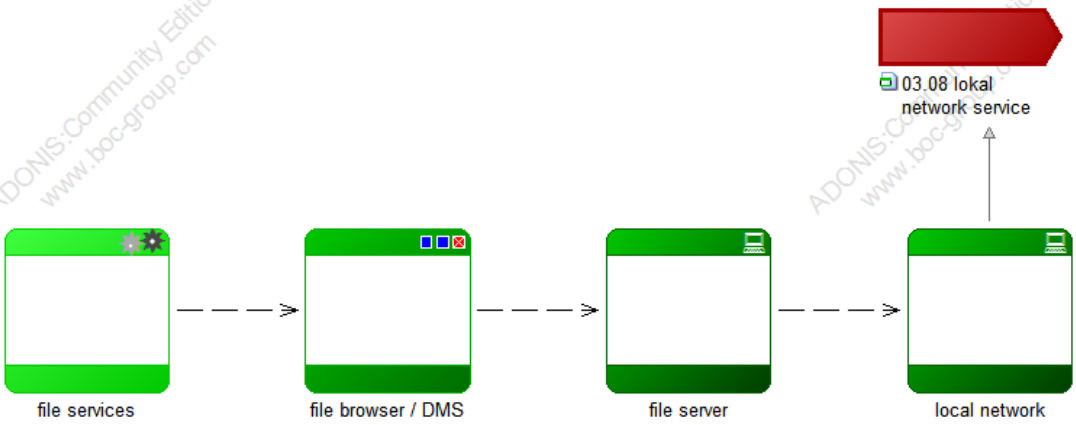


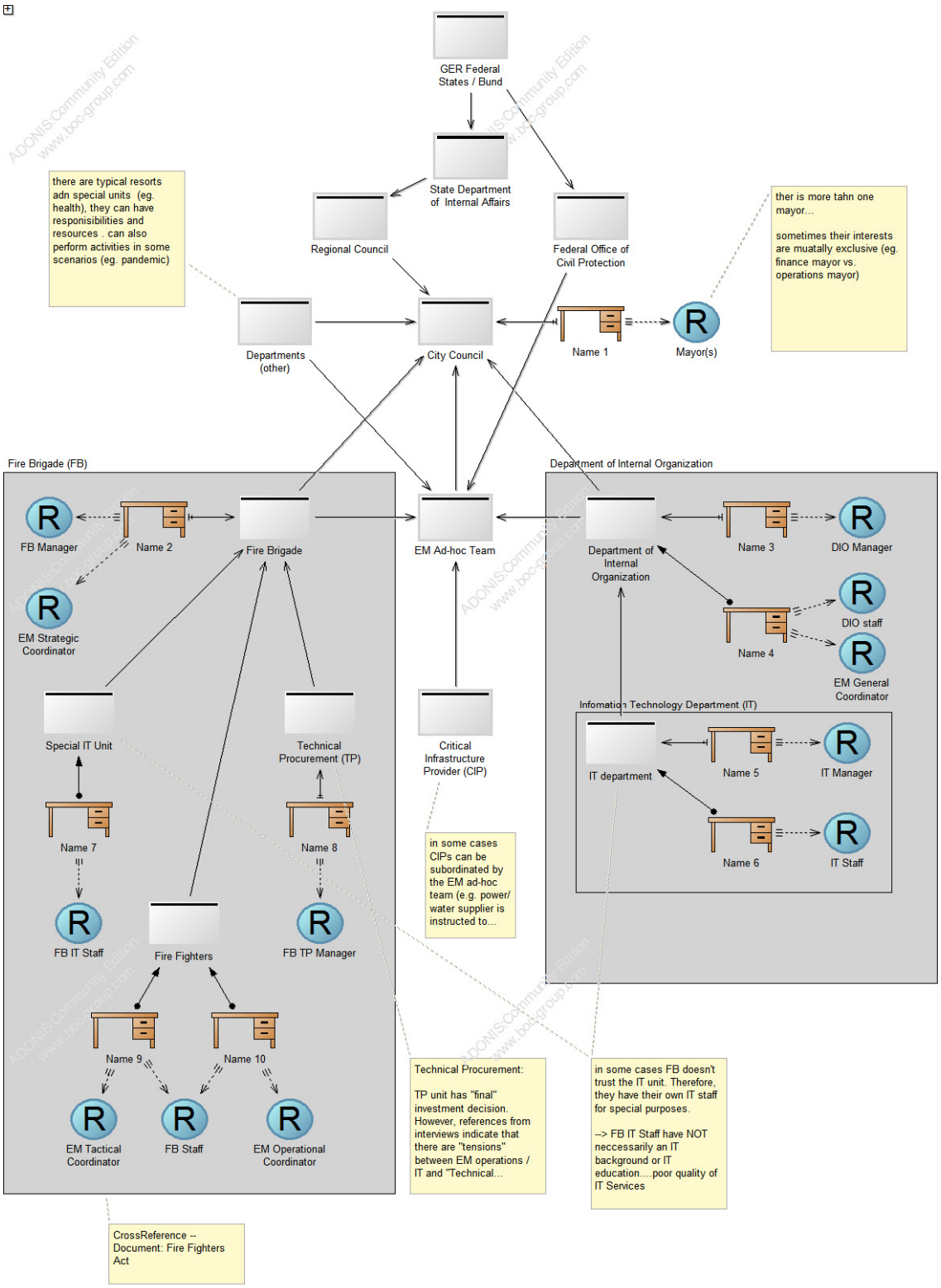


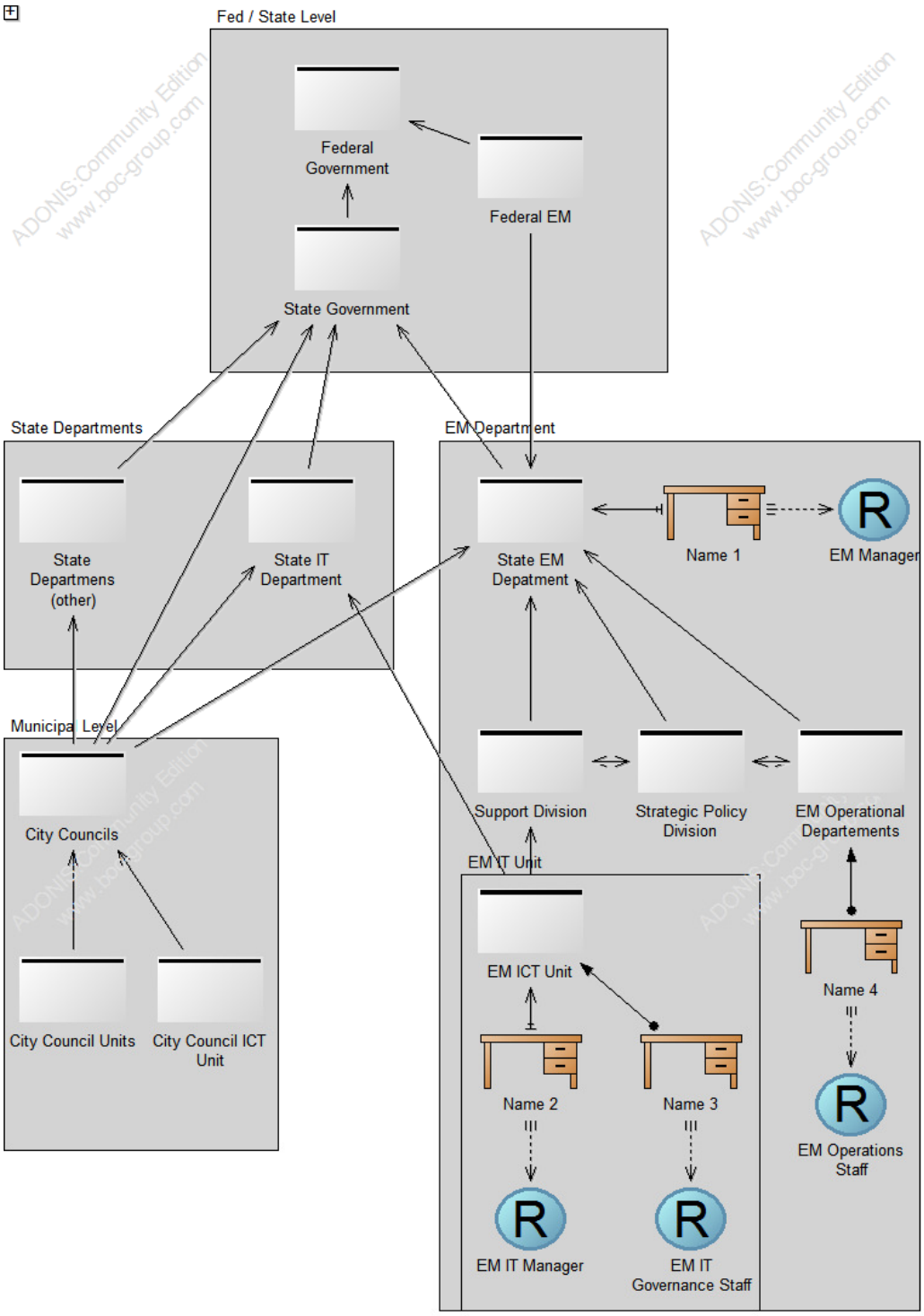


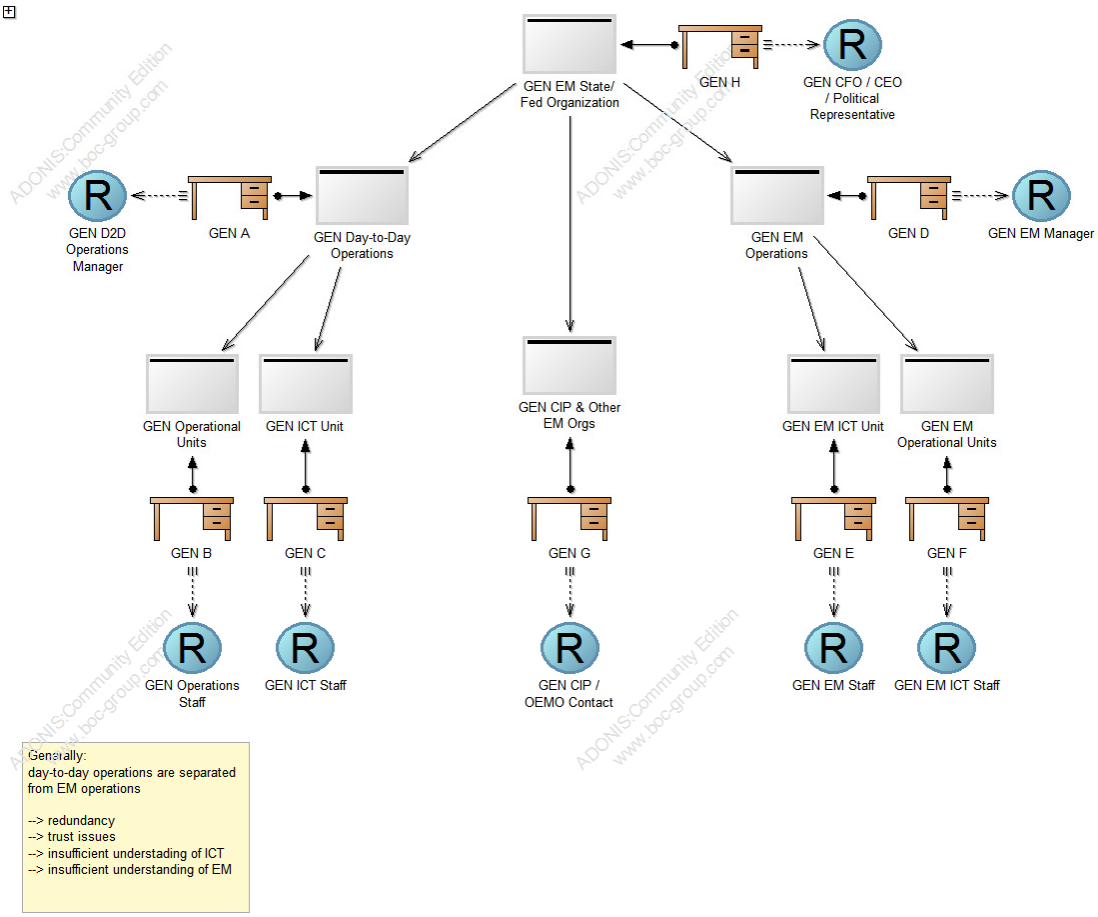

06.01 documents (transfer)
Infrastructure Management (inventarization / monitoring)
Infrastructure Management Server
multiple assets (server, pc, software, etc...)
ICT management tools
Cost Management (ERP)
ERP server
lokal network
03.08 lokal network service
Project Management
file server
03.09 file services

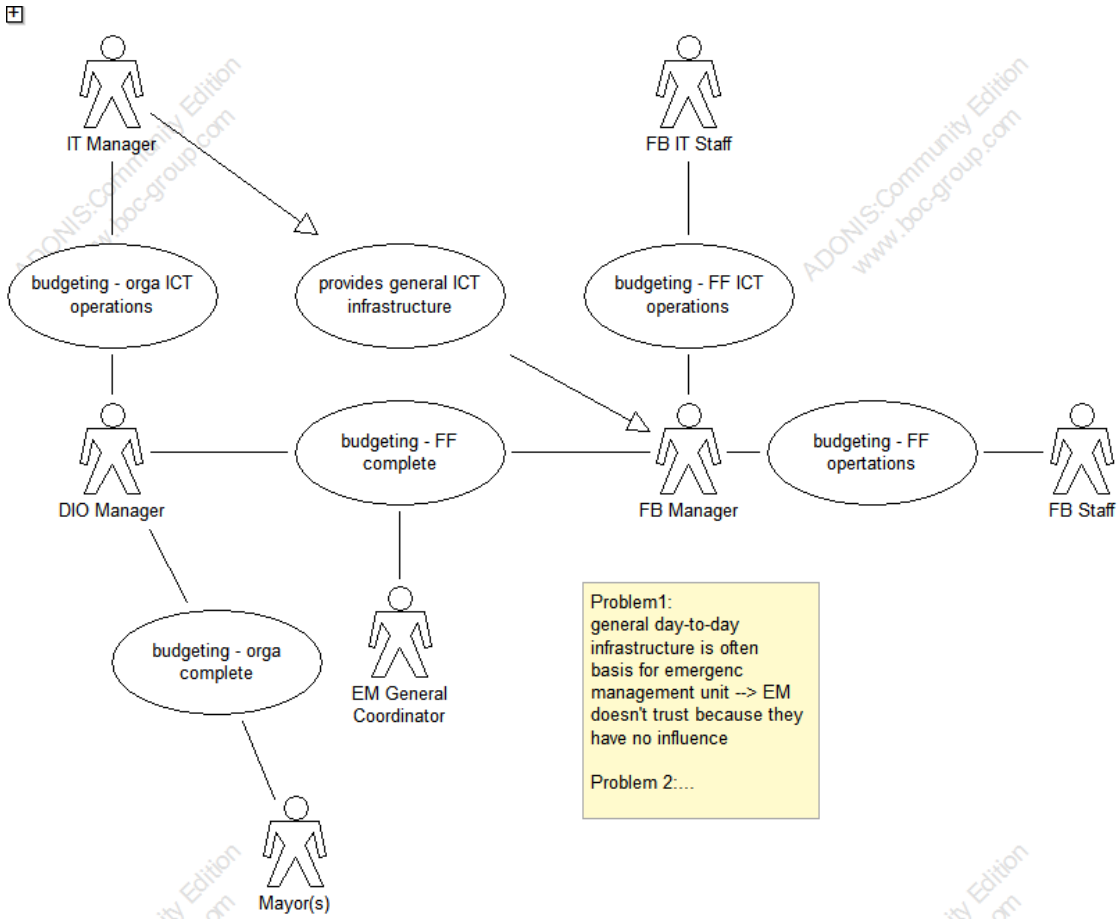


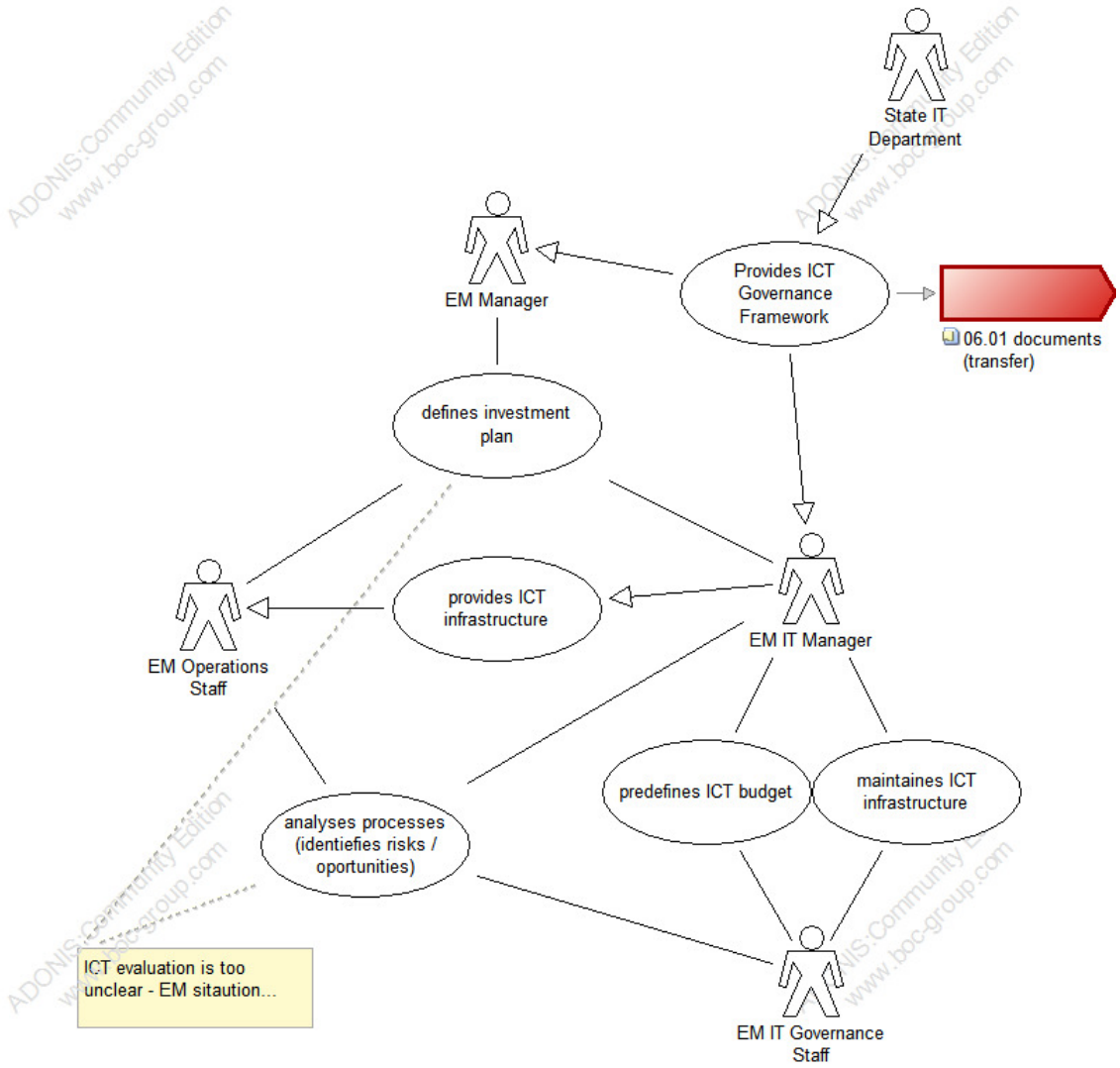


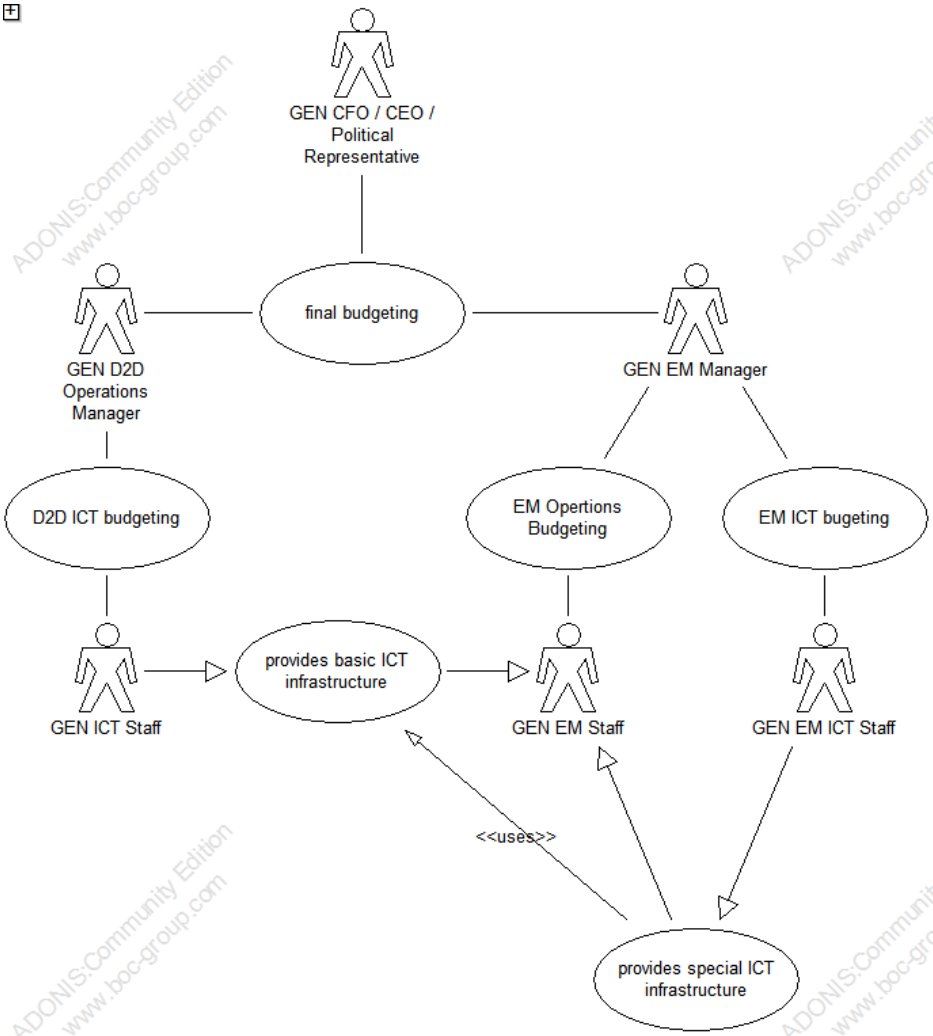

GER Federal States / Bund
State Department of Internal Affairs
Regional Council
Federal Office of Civil Protection
there are typical resorts adn special units (eg. health), they can have responisibilities and resources . can also perform activities in some scenarios (eg. pandemic)
ther is more tahn one mayor...
sometimes their interests are muatally exclusive (eg. finance mayor vs. operations mayor)
Departments (other)
City Council
Name 1
Mayor(s)
Fire Brigade (FB)
Department of Internal Organization
FB Manager
Name 2
Fire Brigade
EM Ad-hoc Team
Department of Internal Organization
Name 3
DIO Manager
DIO staff
Name 4
EM General Coordinator
EM Strategic Coordinator
Special IT Unit
Technical Procurement (TP)
Critical Infrastructure Provider (CIP)
Infomation Technology Department (IT)
IT department
Name 5
IT Manager
Name 6
IT Staff
Name 7
Name 8
FB IT Staff
Fire Fighters
FB TP Manager
in some cases CIPs can be subordinated by the EM ad-hoc team (e.g. power/ water supplier is instructed to...
Name 9
Name 10
EM Tactical Coordinator
FB Staff
EM Operational Coordinator
Technical Procurement:
TP unit has "final" investment decision. However, references from interviews indicate that there are "tensions" between EM operations / IT and "Technical...
in some cases FB doesn't trust the IT unit. Therefore, they have their own IT staff for special purposes.
--> FB IT Staff have NOT neccessarily an IT background or IT education....poor quality of IT Services
CrossReference -- Document: Fire Fighters Act

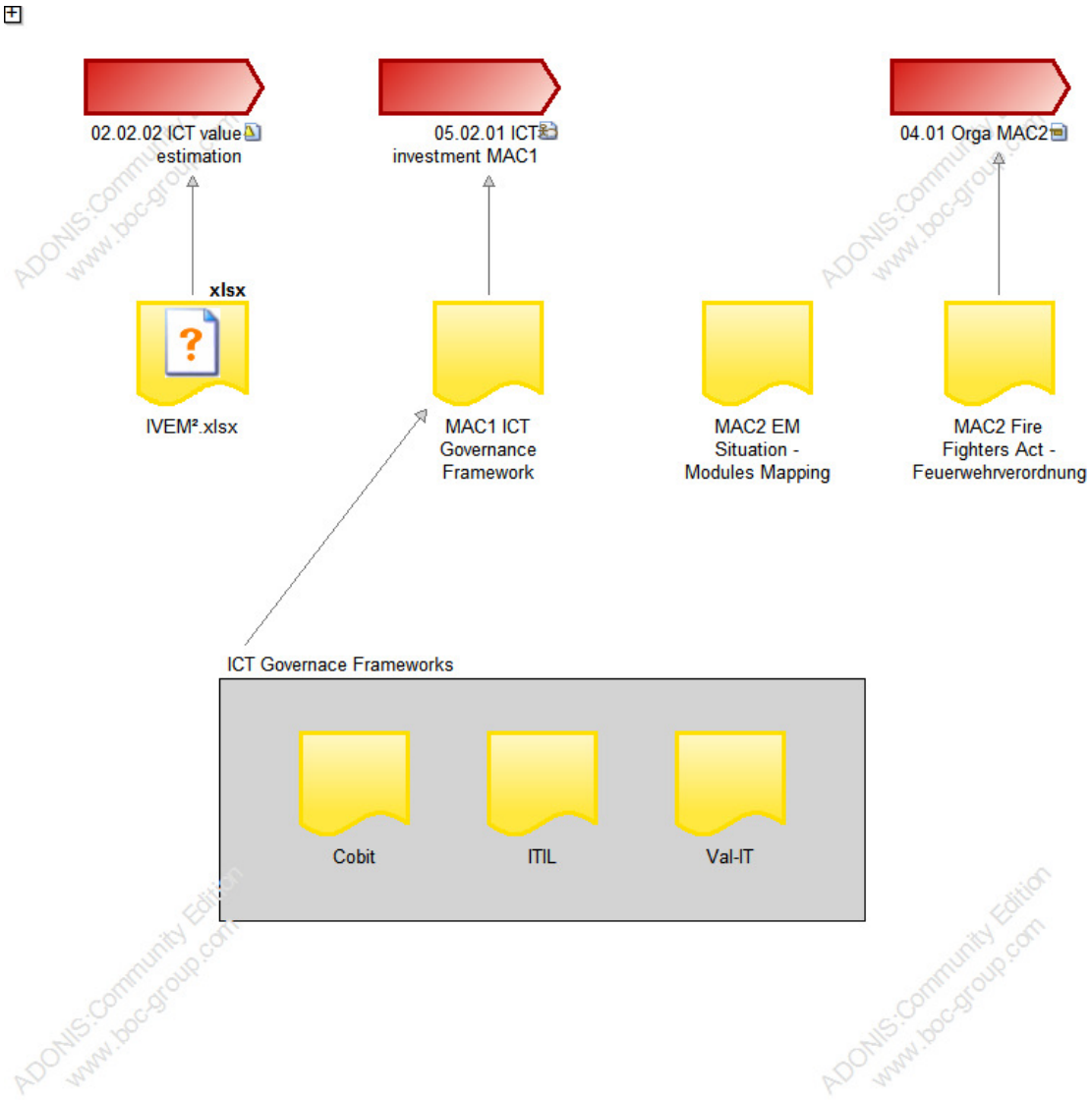

Fed / State Level
Federal Government
Federal EM
State Government
State Departments
State Departmens (other)
State IT Department
EM Department
State EM Depatment
Name 1
EM Manager
Municipal Level
City Councils
City Council Units
City Council ICT Unit
Support Division
Strategic Policy Division
EM Operational Departements
EM IT Unit
EM ICT Unit
Name 2
Name 3
Name 4
EM IT Manager
EM IT Governance Staff
EM Operations Staff

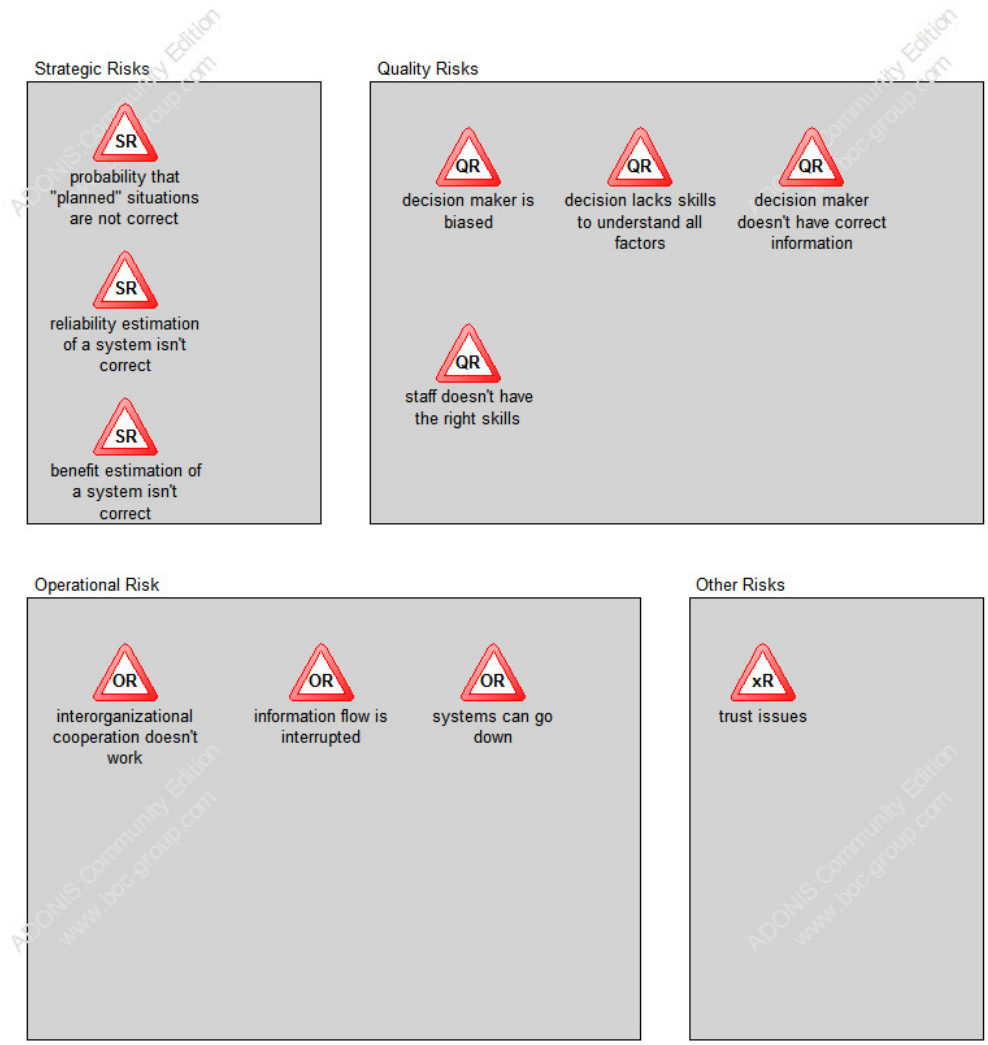

GEN EM State/ Fed Organization
GEN H
GEN CFO / CEO / Political Representative
GEN D2D Operations Manager
GEN A
GEN Day-to-Day Operations
GEN EM Operations
GEN D
GEN EM Manager
GEN Operational Units
GEN ICT Unit
GEN CIP & Other EM Orgs
GEN EM ICT Unit
GEN EM Operational Units
GEN B
GEN C
GEN G
GEN E
GEN F
GEN Operations Staff
GEN ICT Staff
GEN CIP / OEMO Contact
GEN EM Staff
GEN EM ICT Staff
Generally:
day-to-day operations are separated from EM operations
--> redundancy
--> trust issues
--> insufficient understading of ICT
--> insufficient understanding of EM

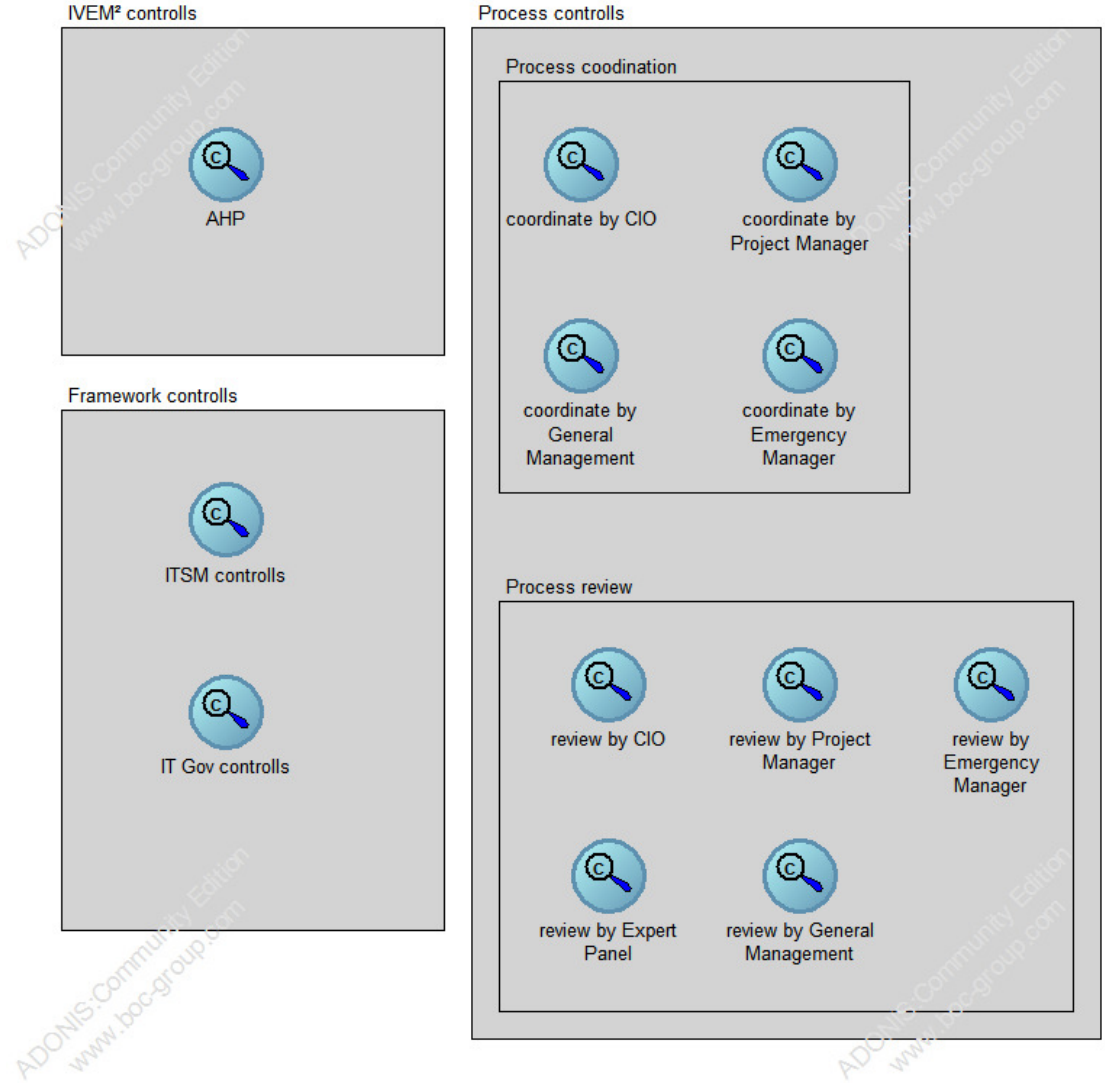

IT Manager
FB IT Staff
budgeting - orga ICT operations
provides general ICT infrastructure
budgeting - FF ICT operations
DIO Manager
budgeting - FF complete
FB Manager
budgeting - FF opertations
FB Staff
budgeting - orga complete
EM General Coordinator
Problem1:
general day-to-day infrastructure is often basis for emergenc management unit --> EM doesn't trust because they have no influence
Problem 2:...
Mayor(s)
ADONIS:Community Edition
www.boc-group.com

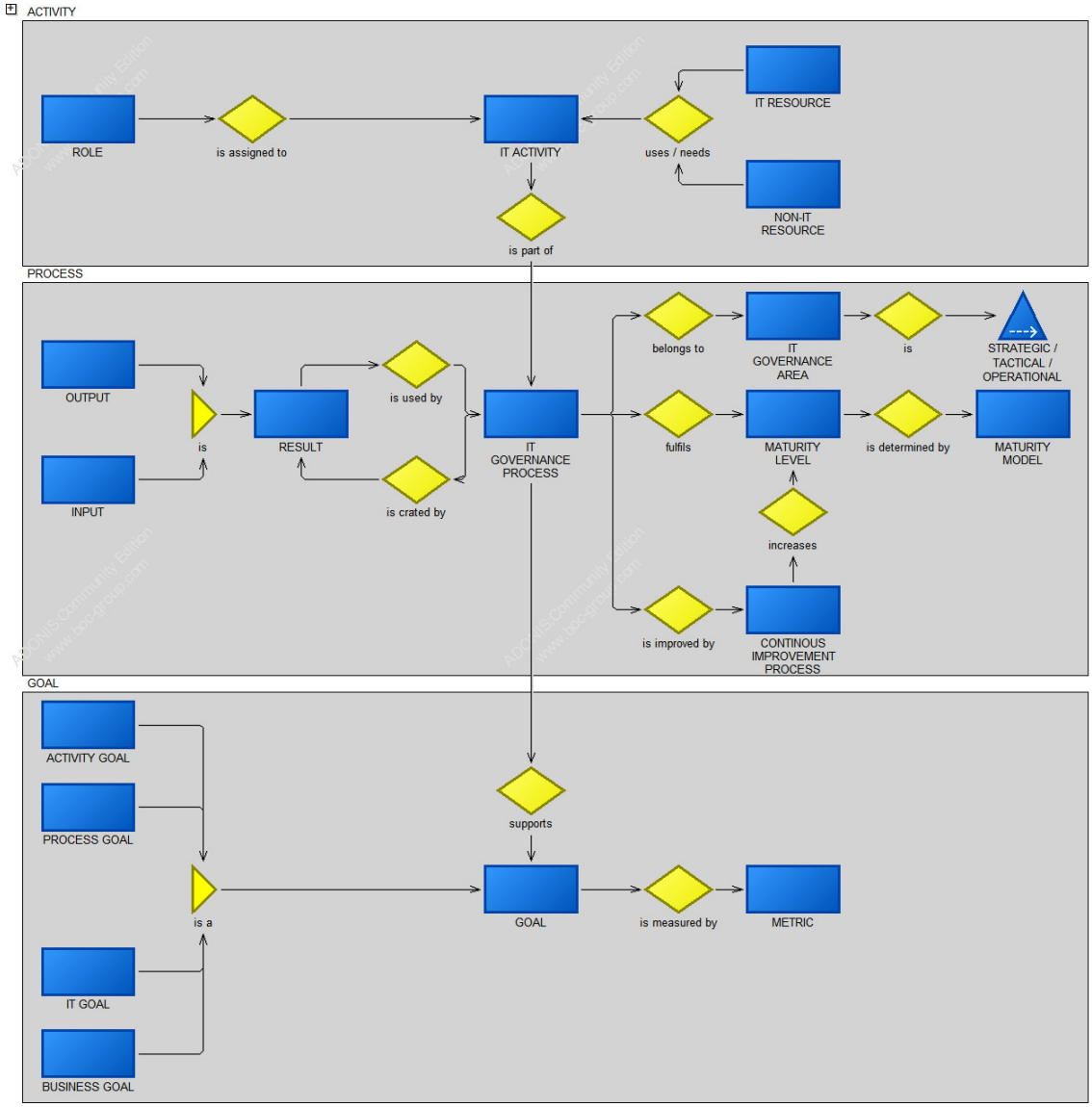

State IT Department
EM Manager
Provides ICT Governance Framework
06.01 documents (transfer)
defines investment plan
EM Operations Staff
provides ICT infrastructure
EM IT Manager
predefines ICT budget
maintaines ICT infrastructure
analyses processes (identiefies risks / oportunities)
ICT evaluation is too unclear - EM sitaution...
EM IT Governance Staff

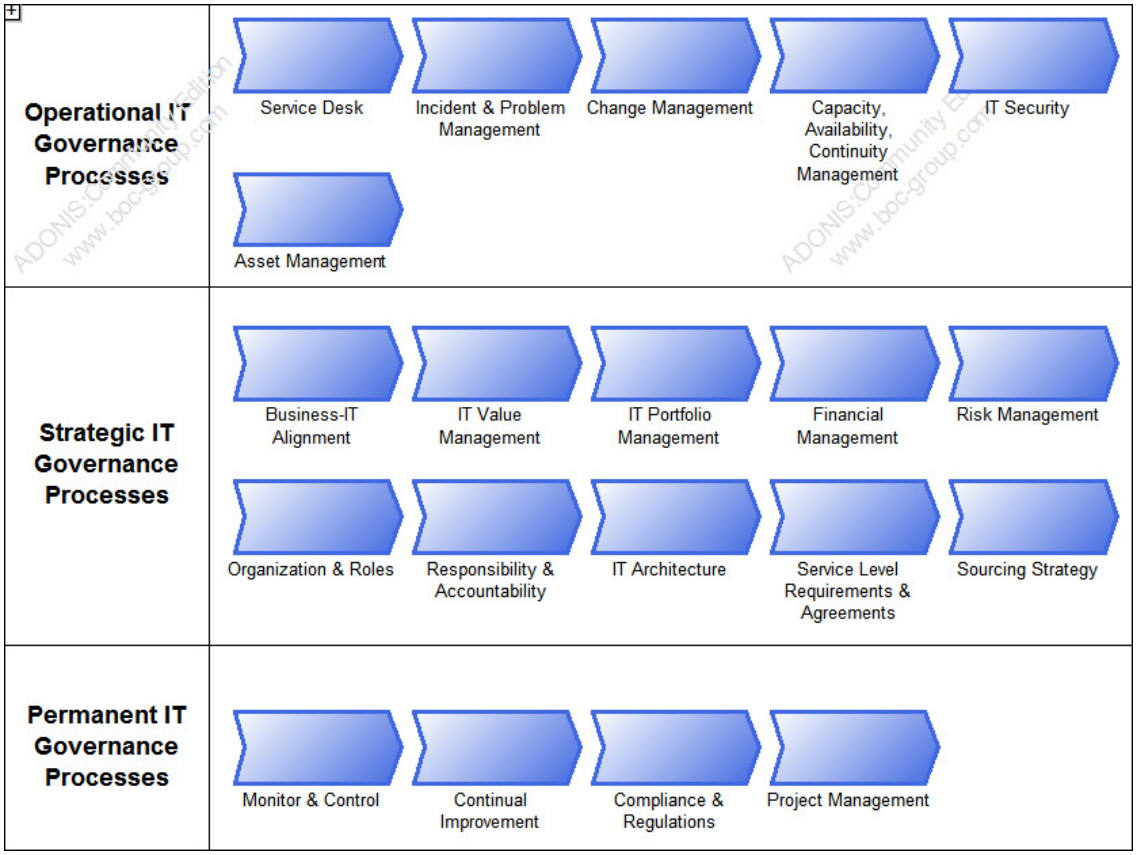

GEN CFO / CEO / Political Representative
final budgeting
GEN D2D Operations Manager
GEN EM Manager
D2D ICT budgeting
EM Opertions Budgeting
EM ICT bugeting
GEN ICT Staff
provides basic ICT infrastructure
GEN EM Staff
GEN EM ICT Staff
<<uses>>
provides special ICT infrastructure
ADONIS:Community Edition
www.boc-group.com


02.02.02 ICT value estimation
05.02.01 ICT investment MAC1
04.01 Orga MAC2
xlsx
IVEM².xlsx
MAC1 ICT Governance Framework
MAC2 EM Situation - Modules Mapping
MAC2 Fire Fighters Act - Feuerwehrverordnung
ICT Governace Frameworks
Cobit
ITIL
Val-IT
ADONIS:Community Edition
www.boc-group.com


Strategic Risks
SR
probability that "planned" situations are not correct
SR
reliability estimation of a system isn't correct
SR
benefit estimation of a system isn't correct
Quality Risks
QR
decision maker is biased
QR
decision lacks skills to understand all factors
QR
decision maker doesn't have correct information
QR
staff doesn't have the right skills
Operational Risk
OR
interorganizational cooperation doesn't work
OR
information flow is interrupted
OR
systems can go down
Other Risks
xR
trust issues


IVEM² controlls
AHP
Framework controlls
ITSM controlls
IT Gov controlls
Process controlls
Process coodination
coordinate by CIO
coordinate by Project Manager
coordinate by General Management
coordinate by Emergency Manager
Process review
review by CIO
review by Project Manager
review by Emergency Manager
review by Expert Panel
review by General Management


ACTIVITY
ROLE
is assigned to
IT ACTIVITY
uses / needs
IT RESOURCE
NON-IT RESOURCE
is part of
PROCESS
OUTPUT
INPUT
is
RESULT
is used by
is crated by
IT GOVERNANCE PROCESS
belongs to
IT GOVERNANCE AREA
is
STRATEGIC / TACTICAL / OPERATIONAL
fulfils
MATURITY LEVEL
is determined by
MATURITY MODEL
increases
is improved by
CONTINOUS IMPROVEMENT PROCESS
GOAL
ACTIVITY GOAL
PROCESS GOAL
IT GOAL
BUSINESS GOAL
is a
supports
GOAL
is measured by
METRIC


Operational IT Governance Processes
Service Desk
Incident & Problem Management
Change Management
Capacity, Availability, Continuity Management
IT Security
Asset Management
Strategic IT Governance Processes
Business-IT Alignment
IT Value Management
IT Portfolio Management
Financial Management
Risk Management
Organization & Roles
Responsibility & Accountability
IT Architecture
Service Level Requirements & Agreements
Sourcing Strategy
Permanent IT Governance Processes
Monitor & Control
Continual Improvement
Compliance & Regulations
Project Management


COBIT controls
Plan & Organize
PO1
PO2
PO3
PO4
PO5
PO6
PO7
PO8
PO9
PO10
Aquire & Implement
AI1
AI2
AI3
AI4
AI5
Deliver & Support
DS1
DS2
DS3
DS4
DS5
DS6
DS7
DS8
DS9
DS10
DS11
DS12
DS13
Monitor & Evaluate
ME1
ME2
ME3
ME4
ITIL controls
Service Strategy
Service Portfolio Management
Demand Management
IT Financial Management
Supplier Management
Service Design
Service Catalogue Management
Service Level Management
Risk Management
Capacity Management
Availability Management
Continuity Management
Security Management
Compliance Management
Architecture Management
Service Operation
Event Management
Incident Management
Problem Management
Request Fulfillment
Access Management
Service Transition
Configuration Management
Validation and Testing
Evaluation
Release and Deplay Mgmt
Cahnge Management
Knowledge Management
Continual Service Improvement
Service Measuring and Reporting
Continual Service Improvement
Val-IT controls
Value Governance
VG1
VG2
VG3
VG4
VG5
VG6
VG7
VG8
VG9
VG10
VG11
Portfolio Management
PM1
PM2
PM3
PM4
PM5
PM6
PM7
PM8
PM9
PM10
PM11
PM12
PM13
PM14
Investment Management
IM1
IM2
IM3
IM4
IM5
IM6
IM7
IM8
IM9
IM10
IM11
IM12
IM13
IM14
IM15

17 Appendix E (Relevant References from the Interviews and Secondary Resources)

“I’m not an IT expert, but the exchange of your IT Management caused that now things are handled differently. What they do is more structured and focused; this certainly helped us to improve our own services”.

“Some people just don’t trust IT because they fear it is unreliable, others won't use IT because they don't understand it…. I understand their position to some degree and I think they are trapped in a circle. Since IT hasn’t much relative importance in most EM organizations, it isn’t managed very well. Consequently, those IT systems are not very reliable. If a system is not reliable it has no or lesser value for EM operations”.

“I think one of our biggest problems is that nobody feels responsible for IT decisions in emergency processes. IT says it’s our baby since they think we have totally different processes compared to the day-to-day business. We know our structures, but we don’t have a clue about IT. That’s an issue if it comes to planning”

“The EM unit is buying things that do not fit into our infrastructure. E.g. they have spent thousands on a high availability system without considering the capabilities of the network and the server room”.

”I wish I could estimate the impact of an investment more rigorously. We’ve spent a lot of money on things that turned out to be less useful”

“Look at the size of these publications. They are just too complex, I don’t have the time to read thousands of pages.”

“EM is different from industry, these frameworks focus too much on monetary goals.”

“A RACI chart is nice for steady procedures, but in emergency situations responsibilities shift depending on the escalation levels.”

“They are not made for “Ad-hoc Teams”.”

“It doesn’t matter if we have a maturity level of 5 if the organizations I work with don’t even know what a “maturity level” is.”

“I’m a Fire-fighter not a Hacker, the terminology used doesn’t relate to my daily work. I would need something more tangible.”

“We use ITIL and Cobit, because we have to by regulations – but we use it only on paper. We are first responders, we do not have time or resources to make differences between an “incident” and a “problem” – things have to work, period. Guidance on how to run IT is good, but these things need to be tailored and I don’t have the time.”

”I believe some of these IT Governance methods are ok, but we had bad experience with other things which are not made for our purposes”

“Yes, we use ITIL and COBIT in our organization, but not for the EM unit, the controls seem too rigid and inflexible for their purpose… so they have a special status”

“IT is interesting, but we don’t have the capacity”

“We are just too small and technologies are too complex”

“In terms of IT we have to rely on the experience of the larger fire-brigades or the academies”.

“Yes, EM uses IT, but nobody really cares about IT issues since the relevant processes are still paper based”

“I think IT is just not reliable enough for our purpose in EM. How can I know that these systems are working if they have to?”

”Nobody feels responsible unless things don’t work and then everybody wants a say”

“I’m pretty sure I could have designed the system. It would work in an emergency if I would know the requirements, but EM didn’t really know what they needed, so on what basis should I design it?”

“EM gets everything they ask for! That’s not the best approach, but we do not want to put lives as stake and we just don’t know better”

“’We are not involved unless the situation has escalated to our level…but then we have to deal with the situation…problem being is, we would need their operations and infrastructure to react effectively and efficiently, but our systems often do not fit to theirs, that’s the reason why we still have to use conventional procedures”

“Also, EP&R has not fully updated its enterprise architecture to govern the IT environment. As a result, during significant disaster response and recovery

operations, such as the 2004 hurricanes, IT systems cannot effectively handle increased workloads, are not adaptable to change, and lack needed real-time reporting capabilities. Such problems usually are due to FEMA's focus on short-term IT fixes rather than long-term solutions. Inadequate requirements definition, alternatives analysis, and testing prior to systems deployment are characteristics of this reactive IT Management approach."(Department of Homeland Security (DHS), 2005, p. 8)

"We don't do any organised data collection now, we just try to solve the problems that come up." (Weyns & Höst 2009, p. 3)

"The IT personnel should get better at defining the limits of their area of responsibility to make sure that the responsibility is where it should be. This is necessary to avoid that the focus lies with the technology instead of the processes." (Weyns & Höst 2009, pp. 3-4)

"Assuring the quality of our IT systems is more difficult. We have discussed this a lot, also with our IT technicians, but they often focus on the wrong things." (Weyns & Höst 2009, p. 4)

"If the IT department can explicitly state that they cannot give us any guarantees, we can justify investing some extra millions ourselves to secure our systems. But without any defined service levels, we have no arguments to justify this cost here." (Weyns & Höst 2009, p. 5)

"Even the service level agreements with external suppliers are often not well planned and not adapted to the level of quality actually demanded by the users of the systems." (Weyns & Höst 2009, p. 5)

“Emergency managers would like to include these systems, but they do not manage to do so because of problems in cooperating with the IT department” (Weyns & Höst 2009, p. 5)

“We are not involved in making emergency plans. It's not something we think about. And I don't know what the rules are for prioritised service in an emergency. Nobody told me whether one computer is more important than another.” (Weyns & Höst 2009, p. 5)

“The committee concluded that IT has as-yet-unrealized potential to improve how communities, the nation, and the global community handle disasters. … Disaster management organizations have not fully exploited many of today’s technology opportunities. This situation stands in contrast to the considerable success enjoyed by some sectors such as financial services and transportation in adopting new IT technologies routinely and aggressively.” (Rao et al. 2007, p.2)

“Disasters are low-frequency events outside the normal planning horizons of most organizations, whose structure, operations, and IT systems are designed to ensure day-to-day efficiency rather than the resilience and scalability that disasters demand. As a result, current research and development efforts may not necessarily focus on developing IT capabilities in a manner optimized for disaster management.” (Rao et al. 2007, p.4)

“A clear vision of end-user goals, a detailed understanding of the individual pieces of the problem and their interrelationships, a detailed understanding of the required technologies, and defined paths for progress would help greatly to inform investment decisions”. (Rao et al. 2007, p.7)

“Often technologies have been acquired as stand-alone products with little consideration for how they integrate with other technologies already in use, even within the same agency” (Rao et al. 2007, p.9)

“In most agencies with disaster management responsibilities, there is no person or unit specifically charged with tracking IT, identifying promising technologies, integrating them into operations, and interacting with IT vendors to make sure needs are addressed.” (Rao et al. 2007, p.69)

“There must be an understanding of the benefits that are obtainable. Weighing the benefits from particular IT investments against the returns on other sorts of investment is challenging. Although having measures of effectiveness is necessary to making such assessments, few applicable metrics are currently available. Above all, acquisition of IT and associated organizational changes should be driven by a focus on improving the effectiveness of those whose actions are integral to effective disaster management. The emphasis should be on measuring the resulting net effectiveness of disaster management activities, not the performance of the IT per se.” (Rao et al. 2007, p.73)

18 Appendix F (ITCO4EM-ITIL-COBIT Mapping)

Level	*Phase*	*ITICO4EM Main Processes*	*ITICO4EM Detailed Processes*	*ITIL Main Processes & Sub-Processes*	*COBIT Processes & Controlled Objectives*
Strategic Level	Prevention	Business / IT Alignment & Value Identification	SL 0.1 Establish a mindset of "IT as an enabler" for EM services SL 0.2 Foster to think in IT services rather than IT technology SL 0.3 Establish a transparent IT Governance which enables EM operations to steer and therefore trust IT SL 1.1 Define and document strategic goals of the organization SL 1.2 Identify threatening scenarios and their likelihood SL 1.3 Identify recurring prevention and countermeasure processes SL 1.4 Identify operation's needs SL 2.1 Identify the value of IT towards recurring processes and/or scenarios SL 2.2 Align IT initiatives with your strategic goals using information about their value, risks and costs and build a prioritized IT portfolio SL 2.3 Ensure balance, long-term value and reusability of IT initiatives	SS 2.1 What is service management SS 2.2 What are services SS 2.3 The business process SS 2.4 Principles of service management SS 3.1 Value creation SS 3.5 Service strategy fundamentals SS 4.1 Define the market SS 4.2 Develop the offerings SS 4.4 Prepare for execution SS 5.1 Financial management SS 5.2 Return on investment SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods SS 5.5 Demand Management SS 6.5 Sourcing strategy SS 7.2 Strategy and design SS 7.3 Strategy and transition SS 7.4 Strategy and operations SS 9.3 Preserving value SD 3.4 Identifying and documenting business requirements and drivers SD 8.1 Business impact analysis	PO 1.1 IT value management PO 1.2 Business-IT alignment PO 1.3 Assessment of current capabilities PO 1.4 IT strategic plan PO 1.5 IT tactical plans PO 1.6 IT portfolio management PO 5.2 Prioritization within IT budget PO 5.4 Cost management PO 5.5 Benefit management PO 8.4 Customer focus ME 4.1 Establishment of an IT Governance framework ME 4.2 Strategic Alignment ME 4.3 Value delivery ME 4.4 Resource management
		Define Responsibilities & Decision Rights	SL 3.1 Involve EM operations in IT decisions to ensure strategic alignment SL 3.2 Involve IT in EM process design to ensure efficient and effective process support SL 3.3 Implement a Crisis Information Officer (CrIO) who co-ordinates between IT initiatives and EM operations and supervises strategic, tactic, and operational goals SL 3.4 Implement an IT Governance board to steer IT initiatives and strategic directions from an EM perspective SL 4.1 Consider shifting organizational structures and decision rights. Ensure that all possible "process owners" are involved in decisions about the design and service levels requirements of IT initiatives SL 4.2 Establish inter-organizational IT co-ordination committees to streamline inter-organizational processes and optimize IT services and infrastructures for a robust, effective and efficient information flow	SS 2.6 Functions across the lifecycle SS 6.1 Organizational development SS 6.3 Organizational design SS 6.4 Organizational culture SS 6.5 Sourcing strategy SD 2.3 Functions and processes across the lifecycle SD 6.1 Functional roles analysis SD 6.4 Roles and Responsibilities ST 6.1 Generic roles ST 6.3 Organizational models to support service transition SO 2.3 Functions across the lifecycle SO 3.1 Functions, groups, teams, departments and divisions SO 3.2 Reactive vs. proactive organizations SO 3.4 Operation staff involvement in service design and service transition	RACI Process Controls (PC2, PC3, P4) PO 3.5 IT architecture board PO 4.2 IT strategy committee PO 4.3 IT steering committee PO 4.4 Organizational placement of the IT function PO 4.5 IT organizational structure PO 4.6 Establishment of roles and responsibilities PO 4.7 Responsibility for IT quality PO 4.8 Responsibility for risk, security and compliance PO 4.9 Data and system ownership DS 4.7 Distribution of the IT continuity plan

		IT Strategy & Enterprise Architecture	SL 5.1 Establish a foresighted and service oriented enterprise architecture, which suites current EM operational needs but also considers future trends and developments SL 5.2 Ensure that all repeatable IT and EM processes are known and documented SL 5.3 Identify and document detailed IT and EM process requirements and limitations SL 5.4 Ensure that current and future availability, capacity, security and continuity requirements are known and considered SL 5.5 Establish standards and quality practices	SS 8.1 Service automation SD 3.3 Identify service requirements SD 3.4 Identifying and documenting business requirements and drivers SD 3.6 Design aspects SD 3.9 Service-oriented architecture SD 3.10 Business service management SD 4.1 Service catalogue management SD 4.3 Capacity management SD 4.4 Availability management SD 4.5 IT service continuity management SD 4.6 Information security management SD 5.2 Data and information management SD 5.3 Application management SO 5.6 Storage and archive	PO 2.1 Enterprise information architecture model PO 3.3 Monitor future trends and regulations PO 4.1 IT Process Framework PO 8.2 IT standards and quality practices AI 1.1 Definition and maintenance of business functional and technical requirements AI 2.1 High-level design AI 2.2 Detailed design AI 3.1 Technological infrastructure acquisition plan AI 4.1 Planning for operational solutions DS 3.1 Performance and capacity planning DS 4.4 Maintenance of the IT continuity plan DS 4.9 Offsite backup storage DS 5.2 IT security plan DS 11.1 Business requirements for data management DS 11.2 Storage and retention arrangements DS 12.4 Protection against environmental factors
		Risk Identification & Management	SL 6.1 Establish and maintain a catalogue of the most crucial EM processes and their associated IT services and IT infrastructuresSL 6.2 Establish an maintain a risk catalogue, which considers possible threats to IT initiatives, IT services and IT infrastructuresSL 6.3 Develop a risk assessment procedure including the major stakeholders and schedules for reassessmentSL 6.4 Assess and manage supplier and service provider risks	SS 9.5 RisksSD 8.3 Risks to the services and processes	PO 9.1 IT risk management frameworkPO 9.3 Event identificationPO 9.4 Risk assessmentPO 9.5 Risk responseAI 1.2 Risk analysis reportDS 2.3 Supplier risk managementME 4.5 Risk management
	Prevention / Preparation	IT Service Level Requirements & Agreements	SL 7.1 Define a service catalogue of retired, offered and planned IT services SL 7.2 Determine service level requirements of offered and planned IT services based on capacity, availability and continuity indicators SL 7.3 Define operating and service level agreements based on requirements and capability of IT infrastructure and IT staff SL 7.4 Define "fallback" processes for critical services and IT resources to ensure "off-line" procedures	SLA OLA SD 4.1 Service catalogue management SD 4.2 Service level management SD 4.3 Capacity management SD 4.4 Availability management SD 4.5 IT service continuity management SD 8.2 Service level requirements	DS 1.1 Service level management framework DS 1.2 Definition of Services DS 1.3 Service level agreements DS 1.4 Operating level agreements DS 3.4 IT resources availability DS 4.1 IT continuity framework DS 4.2 IT continuity plans DS 4.3 Critical IT resources DS 4.8 IT services recovery and resumption
		IT Security	SL 8.1 Implement IT security management and revise IT initiatives on a regular basis SL 8.2 Secure physical and digital access to IT infrastructures and data SL 8.3 Ensure the integrity of identity and information SL 8.4 Establish different levels of security and categorize sensitive data SL 8.5 Define and provide secure and reliable information exchange interfaces based on common standards	SD 4.6 Information security management SO 4.5 Access management SO 5.13 Information security management and operation	PO 2.4 Integrity management DS 5.1 Management of IT security DS 5.2 IT security plan DS 5.3 Identity management DS 5.6 Security incident definition DS 5.8 Cryptographic key management DS 5.11 Exchange of sensitive data DS 11.6 Security requirements for data management DS 12.2 Physical security measures DS 12.3 Physical access DS 13.4 Sensitive documents and output devices AI 3.2 Infrastructure resource protection and availability

		Technology & Service Procurement	SL 9.1 Assess your sourcing capabilities and define your sourcing strategy SL 9.2 Identify all external dependencies and suppliers in order to streamline them and reduce supply shortage and delivery delay SL 9.3 Manage and assess suppliers and service providers to strengthen and/or establish a long-term relationship in order to increase effectiveness and efficiency SL 9.4 Identify and implement co-sourcing possibilities on an inter-organizational level	SS 6.5 Sourcing strategy SD 3.7 Subsequent design activities SD 4.2 Service level management SD 4.7 Supplier management	AI 5.1 Procurement control AI 5.2 Supplier contract management AI 5.3 Supplier selection DS 2.1 Identification of supplier relationships DS 2.2 Supplier relationship management
Strategic / Operational Level	Preparation / Response	Ad-Hoc IT Service Level Requirements & Agreements	SO 1.1 Iteratively use and adapt emergency change procedures (AC 2.2) for urgent requirement and agreement changes SO 1.2 Assess upcoming events for new requirements SO 1.3 Providently inform all stakeholders about possible increase of required resources or availability of services	ST 4.2 Change management	AI 6.3 Emergency changes
		Ad-Hoc IT Security	SO 2.1 Iteratively use and adapt emergency change procedures (AC 2.2) for security changes SO 2.2 Assess upcoming events for required security policy changes SO 2.3 Establish a " inter-organizational security taskforce" to provide ad-hoc and secure information access	ST 4.2 Change management	AI 6.3 Emergency changes
		Ad-Hoc Technology & Service Procurement	SO 3.1 Iteratively use and adapt emergency change procedures (AC 2.2) for urgent technology and service procurements SO 3.2 Assess ad-hoc requirements (SO 1.2) for additional need of technologies or services SO 3.3 Check on inter-organizational level for quick co-sourcing possibilities SO 3.4 Providently inform all suppliers about possible increase of additionally needed technologies or services and negotiate preliminary terms and conditions	ST 4.2 Change management	AI 6.3 Emergency changes

OperationalLevel	Response /Recovery	Service & Infrastructure operations - Keep "IT" running	OL 1.1 Establish a service desk for incident, event and request handlingOL 1.2 Prioritize incidents, events, and requests based on process impactOL 1.3 Identify and execute emergency changes based on process impactOL 1.4 Implement effective and efficient escalation routinesOL 2.1 Use a configuration repository to collect and retrieve information about IT services and IT assetsOL 2.2 Document necessary changes, solutions and closuresOL 3.1 Proactively maintain critical servers, networks, software and fallback systemsOL 3.2 Co-maintain inter-organizational services and interfaces	CMDBSD 4.3 Capacity managementSD 4.4 Availability managementSD 4.5 IT service continuity managementST 4.2 Change managementST 4.3 Service asset and configuration managementST 4.4 Release and deploy managementSO 2.4 Service operation fundamentalsSO 3.3 Providing serviceSO 3.5 Operational healthSO 3.7 DocumentationSO 4.1 Event managementSO 4.2 Incident managementSO 4.3 Request FulfillmentSO 4.6 Operational activities covered in other lifecycle phasesSO 5.2 IT operationsSO 5.4 Server management and supportSO 5.5 Network managementSO 5.7 Database administrationSO 5.8 Directory services managementSO 5.9 Desktop supportSO 5.10 Middleware managementSO 5.12 Facilities and data center managementSO 5.11 Internet/Web managementSO 6.2 Service deskSO 6.4 IT operations management	AI 3.2 Infrastructure resource protection and availabilityAI 3.3 Infrastructure maintenanceAI 6.3 Emergency changesDS 3.4 IT resources availabilityDS 4.1 IT continuity frameworkDS 4.2 IT continuity plansDS 4.3 Critical IT resourcesDS 4.8 IT services recovery and resumptionDS 5.7 Protection of security technologyDS 5.9 Malicious software prevention, detection and correctionDS 8.1 Service deskDS 8.2 Registration of customer queriesDS 8.3 Incident escalationDS 8.4 Incident closureDS 9.1 Configuration repository and baselineDS 9.2 Identification and maintenance of configuration itemsDS 13.1 Operations procedures and instructionsDS 13.5 Preventive maintenance for hardware
Audit & Control	All / Transition & Improvement	Monitor, Control & Improve	AC 1.1 Define key performance indicators to measure the performance of your processes and IT infrastructure AC 1.2 Measure and assess your processes and IT infrastructure AC 1.3 Report your performance to the IT Governance board AC 1.4 Implement and follow a continual improvement process AC 1.5 Review incidents and events during operation to identify recurring patterns	SD 4.3 Capacity management SD 4.4 Availability management SD 8.5 Measurement of service design SO 3.6 Operational health SO 4.4 Problem management SO 5.1 Monitor and control CSI 3.10 Governance CSI 4.1 Seven step improvement process CSI 4.2 Service reporting CSI 4.3 Service measurement CSI 5.2 Assessments CSI 5.3 Benchmarking CSI 5.4 Measuring and reporting frameworks CSI 5.5 Deming cycle CSI 6 Organizing for continual service improvement	PO 8.1 Quality management system PO 8.5 Continuous Improvement PO 8.6 Quality measurement, monitoring and review DS 1.5 Monitoring and reporting of service level achievements DS 1.6 Review of service level agreements and contracts DS 2.4 Supplier performance monitoring DS 3.2 Current performance and capacity DS 3.3 Future performance and capacity DS 3.4 IT resources availability DS 3.5 Monitoring and reporting DS 10.1 Identification and classification of problems DS 10.2 Problem tracking and resolution DS 10.3 Problem closure DS 13.3 IT infrastructure monitoring ME 1.1 Monitoring approach ME 1.2 Definition of collection of monitoring data ME 1.3 Monitoring method ME 1.4 Performance assessment ME 1.5 Board and executive reporting ME 4.6 Performance measurement AI 7.9 Post-implementation review

		Change Management	AC 2.1 Implement change standards and proceduresAC 2.2 Implement emergency change proceduresAC 2.3 Provide guidelines for change assessment and prioritizationAC 2.4 Test and authorize changesAC 2.5 Release and deploy changesAC 2.6 Evaluate changes madeAC 2.7 Document changes and update the configuration repository	ST 3.1 Principles supporting service transitionST 3.2 Policies for service transitionST 4.1 Transition planning and supportST 4.2 Change ManagementST 4.3 Service asset and configuration managementST 4.4 Release and deployment managementST 4.5 Service validation and testingST 4.6 Evaluation	PO 8.2 IT standards and quality practicesDS 9.1 Configuration repository and baselineAI 3.4 Feasibility test environmentAI 6.1 Change standards and proceduresAI 6.2 Impact assessment, prioritization and authorizationAI 6.3 Emergency changesAI 6.4 Change status tracking and reportingAI 6.5 Change closure and documentationAI 7.2 Test planAI 7.3 Implementation planAI 7.4 Test environment
	All / Regulations	Compliance & Regulations	AC 3.1 Identify legal, regulatory, and contractual compliance requirements AC 3.2 Evaluate compliance of IT supported processes and services AC 3.3 Improve compliance with existing regulations and pro-actively influence new regulations to optimize IT driven EM procedures	no specific" compliance management process"	ME 3.1 Identification of external legal, regulatory and contractual compliance requirements ME 3.2 Optimization of response to external requirements ME 3.3 Evaluation of compliance with external requirements
	All / Projects & Collaboration	Project & Program Management	AC 4.1 Establish a "P3" (project, programme, portfolio) mindset and approach AC 4.2 Implement a project management framework to manage scope, risk and implementation	ST 3.2 Policies for service transition	PO 10.1 Programme management framework PO 10.2 Project management framework PO 10.3 Project management approach PO 10.4 Stakeholder commitment PO 10.5 Project scope statement PO 10.8 Integrated project plan PO 10.9 Project risk management PO 10.13 Project performance measurement, reporting and monitoring AI1.3 Feasibility study and formulation of alternative courses of action
		Inter-Organizational Collaboration & Service Integration	AC 5.1 Define information exchange procedures AC 5.2 Define inter-organizational security procedures AC 5.3 Establish inter-organizational IT cooperation AC 5.4 Provide and maintain an inter-organizational kowledge and adress database for key-staff and key-functions AC 5.5 Establish and use mutual IT standards AC 5.6 Consider a purchasing association with close partners	SO 4.5 Access management	DS 5.3 Identity management DS 5.8 Cryptographic key management DS 5.10 Exchange of sensitive data

Abbreviations:	ITICO4EM Levels	ITIL Books	COBIT Domains
	SL = Strategic Level	SS = Service Strategy	PO = Plan & Organize
	SO = Strategic / Operational Level	SD = Service Design	ME = Monitor & Evaluate
	OL = Operational Level	ST = Service Transition	AI = Acquire & Implement
	AC = Audit & Control Level	SO = Service Operation	DS = Deliver & Support
		CSI = Continual Service Improvement	

19 Appendix G (ITCO4EM – Detailed Processes)

ProcessLevel	EMPhase	ITICO4EMProcesses	ITICO4EMDetailed Processes - Explanation
Strategic Level	Prevention	Business / IT Alignment & Value Identification	**SL 0.1 Establish a mindset of "IT as an enabler" for EM services** - Before applying IT Governance methods EM organizations have to establish an understanding of "IT as an enabler" in technical and non-technical units. It has to be understood by non-technical EM units that IT is not a cryptic and unreliable technology but can provide fundamental support and opportunities for EM processes. On the other hand technical units have to understand that IT is not there because EM wants new technology, IT is there because EM wants to improve their EM processes.
			SL 0.2 Foster to think in IT services rather than IT technology - Shift from a technological point of view to a service oriented point of view. An IT service can be understood and evaluated by technical staff as well as non-technical staff. the main goal is to realize the value of IT to the EM process.
			SL 0.3 Establish a transparent IT Governance which enables EM operations to steer and therefore trust IT - IT initiatives should become clear to non-technical steering committee members. It is essential that IT decisions on a high level (e.g. on project, programme, and portfolio) involve non-technical members to increase the acceptance of IT-supported and improved EM processes. Risks and opportunities of IT initiatives have to be presented in non-technical vocabulary to make their impact on the operational processes more transparent.
			SL 1.1 Define and document strategic goals of the organization - It is important to define and document the strategic goals of an EM organization in order to align IT initiatives towards them. Documented strategic goals can be assed and prioritized according to their impact.
			SL 1.2 Identify threatening scenarios and their likelihood - Every EM organization has a different set and likelihood of possible threatening scenarios (e.g. tsunamis are only of concern to EM organizations along the coast line, and the likelihood of tsunamis varies in different coastal regions). Knowing possible scenarios and their likelihood will help to develop the most suitable countermeasures.

			SL 1.3 Identify recurring prevention and countermeasure processes - Identifying recurring prevention and countermeasures processes will help to streamline and optimize EM operations for different scenarios rather than only a few scenarios. E.g. Optimizing EM procedures towards tsunamis and flooding might leave the EM vulnerable to bushfire and nuclear fall-out scenarios. However, by identifying and optimizing processes, which can be reused in different scenarios (e.g. the evacuation process could be reused during flooding, bushfire, fall-out, etc.), an EM organization can remain flexible and high-performing at the same time.
			SL 1.4 Identify operation's needs - It is critical to know EM operations needs in order to design effective and efficient IT services.
			SL 2.1 Identify the value of IT towards recurring processes and/or scenarios- assessing the value of IT initiatives towards recurring EM processes (e.g. evacuation) is easier than to identify the value of IT towards complex or even unknown scenarios.
			SL 2.2 Align IT initiatives with your strategic goals using information about their value, risks and costs and build a prioritized IT portfolio - Resources are usually limited, hence it is important to align IT initiatives towards EM operations. Information about cost, value, and risk of IT initiatives should be used to build an IT portfolio and invest in the most beneficial projects and programmes.
			SL 2.3 Ensure balance, long-term value and reusability of IT initiatives - Ensure that the IT portfolio is balanced and supports opportunistic as well as value conserving IT initiatives. Maintenance or upgrades of existing critical IT infrastructures should not be sacrificed for new IT services.
		Define Responsibilities & Decision Rights	**SL 3.1 Involve EM operations in IT decisions to ensure strategic alignment** - By involving representatives of EM operations in the decision making process, risks and opportunities of IT initiatives towards EM processes can be better assessed from an operation perspective. Hence, IT services can be better aligned to EM operations needs.
			SL 3.2 Involve IT in EM process design to ensure efficient and effective process support - By involving IT staff in the design and/or re-design of EM processes improved technologies and existing enterprise architectures can be considered to ensure efficient and effective process support.

			SL 3.3 Implement a Crisis Information Officer (CrIO) who co-ordinates between IT initiatives and EM operations and supervises strategic, tactic, and operational goals - By the implementation of a Crisis Information Officer a EM organization can ensure that EM and IT initiatives are coordinated. The CrIO has to understand EM options and IT architectures. A CrIO is the leader of the IT Governance steering committee and can mediate between IT and EM operations.
			SL 3.4 Implement an IT Governance board to steer IT initiatives and strategic directions from an EM perspective - By implementing an IT Governance board an EM organizations can ensure that operational, tactical and strategic goals are met by IT initiatives. The steering board should consist of representatives from EM operations and IT to ensure that the portfolio is balanced and serves EM goals.
			SL 4.1 Consider shifting organizational structures and decision rights. Ensure that all possible "process owners" are involved in decisions about the design and service levels requirements of IT initiatives - In some cases decision rights and responsibilities shift when emergency situation escalate, hence decisions made in the "day-to-day" business affect decision made during an emergency situation. To ensure trust in IT infrastructures and IT services all "process owners" should be involved in decision about the design and service quality of IT initiatives and IT services.
			SL 4.2 Establish inter-organizational IT co-ordination committees to streamline inter-organizational processes and optimize IT services and infrastructures for a robust, effective and efficient information flow- Since some emergency situations require the cooperation of different EM organizations and authorities an inter-organizational IT coordination committee should be established to ensure the information flow between organizations and authorities. If possible the inter-organizational committee should steer upcoming IT initiatives towards a direction where IT infrastructures and IT services are compatible or even interchangeable in order to compensate shortcomings or failures during critical EM situations.
		IT Strategy & Enterprise Architecture	**SL 5.1 Establish a foresighted and service oriented enterprise architecture, which suites current EM operational needs but also considers future trends and developments** - To ensure the long-term maintenance of IT value to an EM organization the enterprise architecture should be designed service oriented and consider current and future IT trends.

			SL 5.2 Ensure that all repeatable IT and EM processes are known and documented - In order to design a sustainable enterprise architecture with efficient and effective IT services for the EM operation, all repeatable business process should be known, documented and updated.
			SL 5.3 Identify and document detailed IT and EM process requirements and limitations - To design and assess more efficient and effective IT services detailed circumstances have to be known. Hence current and future requirements and/or limitations have to be identified, documented and updated.
			SL 5.4 Ensure that current and future availability, capacity, security and continuity requirements are known and considered - To ensure sustainability of IT infrastructure investments and IT services technical aspect have to be considered. Hence, predictions about the availability, capacity, security and continuity requirements must influence all IT initiatives.
			SL 5.5 Establish standards and quality practices - Standards ensure compatibility with current and future technologies, their utilization is quick and efficient and they can provides a constant level of quality.
		Risk Identification & Management	**SL 6.1 Establish and maintain a catalogue of the most crucial EM processes and their associated IT services and IT infrastructures** - If the most crucial EM processes are known associated IT services and infrastructures can be managed and maintained pro-actively to ensure their availability and quality.
			SL 6.2 Establish an maintain a risk catalogue, which considers possible threats to IT initiatives, IT services and IT infrastructures - Having a risk catalogue reduces the risk of unconsidered threats. A risk catalogue provides a good guideline to assess new IT initiatives.
			SL 6.3 Develop a risk assessment procedure including the major stakeholders and schedules for reassessment - Having a standard and recurring risk assessment procedure which includes the major stakeholders decreases the likelihood of unidentified risk to existing IT.
			SL 6.4 Assess and manage supplier and service provider risks - By assessing the risks associated with suppliers and service providers the EM organizations is able to prioritize suppliers and providers not only by cost but also by their capabilities and deficiencies, which in turn builds the basis for continual improvements with key suppliers and providers.

	Prevention / Preparation	IT Service Level Requirements & Agreements	**SL 7.1 Define a service catalogue of retired, offered and planned IT services** - To keep track about IT services a catalogue or previous, current and future IT services should be provided and maintained. It is also beneficial to increase transparency of and trust in IT services since EM operations is aware of offered services and their associated service levels.
			SL 7.2 Determine service level requirements of offered and planned IT services based on capacity, availability and continuity indicators - The service catalogue can build a basis for discussion to determine service level parameters such as capacity, availability and continuity requirement.
			SL 7.3 Define operating and service level agreements based on requirements and capability of IT infrastructure and IT staff - Not only requirements by the EM operations should be considers when service levels are agreed, also the capabilities of IT infrastructure and IT staff must be considered.
			SL 7.4 Define "fallback" processes for critical services and IT resources to ensure "off-line" procedures - Ensure that alternative "off-line" procedures are in place for critical IT services and infrastructures. This increases trust of EM operations in IT enabled processes.
		IT Security	**SL 8.1 Implement IT security management and revise IT initiatives on a regular basis** - Secure access to information is crucial for EM operation. Hence, all IT initiatives should be assessed and re-assessed from a security perspective.
			SL 8.2 Secure physical and digital access to IT infrastructures and data - Critical data and IT infrastructures must be protected from unauthorized access. IT security management must be concerned not only with digital but also with physical access to minimize the risk of attacks.
			SL 8.3 Ensure the integrity of identity and information - EM operations rely on correct information, hence IT security management has to ensure the integrity of data and the identity of sender and receiver of information.
			SL 8.4 Establish different levels of security and categorize sensitive data- Not everybody needs access to all information. In order to reduce the impact of compromised accounts and infrastructures IT security management should implement different levels of security and categorize sensitive data accordingly.

			SL 8.5 Define and provide secure and reliable information exchange interfaces based on common standards - due to inter-organizational data exchange IT security management should provide and manage appropriate interfaces and infrastructures to ensure a secure and reliable information flow based on common standards.
		Technology & Service Procurement	**SL 9.1 Assess your sourcing capabilities and define your sourcing strategy** - A EM organization has to know their own sourcing capabilities. Not all IT services can or should be provided by own staff. Hence, a sourcing strategy has to be defined in order to separate between in-, co- and out-sourced IT services.
			SL 9.2 Identify all external dependencies and suppliers in order to streamline them and reduce supply shortage and delivery delay - Co- and out-sourcing can be beneficial but it can also generate dependencies, which might become a bottleneck in emergency situations. Dependencies must be clear in order to realize and reduce associated risks. Critical supply and service chains need to be streamlined and strengthened or backed by alternatives (e.g. second and independent internet connection)
			SL 9.3 Manage and assess suppliers and service providers to strengthen and/or establish a long-term relation ship in order to increase effectiveness and efficiency - Suppliers and service providers have to be assessed according to their capabilities and risks. Weaknesses in the supply chain have to be mutually eliminated and risky suppliers and service provides be replaced. Integration of suppliers and service providers in process designs can be mutually beneficial and increase effectiveness and efficiency.
			SL 9.4 Identify and implement co-sourcing possibilities on an inter-organizational level - It can be beneficial to identify and implement co-sourcing possibilities with other EM organizations in proximity. If EM organizations have to work together on a regular basis this can help to overcome shortages during an emergency situation. (See also AC 5.6 and Ad-Hoc Technology & Service Procurement)
Strategic / Operational Level	Preparation / Response	Ad-Hoc IT Service Level Requirements & Agreements	**SO 1.1 Iteratively use and adapt emergency change procedures (AC 2.2) for urgent requirement and agreement changes** - Emergency situation require a quick but also reliable changes. Unbureaucratic procedures and experiences from previous situations should be used adapt to new situations.
			SO 1.2 Assess upcoming events for new requirements - All emergency situations should be assessed to identify deviations from existing plans or procedures. Possible requirement changes should be identified as early as possible to be able to adapt to new situations.

			SO 1.3 Providently inform all stakeholders about possible increase of required resources or availability of services - Early involvement of all stakeholders will increase the preparedness for deviations and will enable them to find solutions.
		Ad-Hoc IT Security	**SO 2.1 Iteratively use and adapt emergency change procedures (AC 2.2) for security changes**- Emergency situations require EM organizations to access and provide information. In some cases this requires to change security policies or access rights. Unbureaucratic procedures and experiences from previous situations should be used adapt to new situations.
			SO 2.2 Assess upcoming events for required security policy changes - All emergency situations should be assessed to identify possible security changes. These should be identified as early as possible to be able to adapt to new situations.
			SO 2.3 Establish an "inter-organizational security taskforce" to provide ad-hoc and secure information access - Early involvement of key stakeholders and key IT staff in an "inter-organizational security taskforce" will help to make quick and reliable decisions about security policy changes.
		Ad-Hoc Technology & Service Procurement	**SO 3.1 Iteratively use and adapt emergency change procedures (AC 2.2) for urgent technology and service procurements** - Emergency situations can require a additional resources or extra services, which must be purchased ad-hoc in order to respond with the right countermeasures. Unbureaucratic procedures and strong relations with suppliers and providers should be used adapt to new situations.
			SO 3.2 Assess ad-hoc requirements (SO 1.2) for additional need of technologies or services - Identify additional resources and services for new or increased requirements.
			SO 3.3 Check on inter-organizational level for quick co-sourcing possibilities - Use already available resources from close and/or participating EM organizations to save resources and act quickly.
			SO 3.4 Providently inform all suppliers about possible increase of additionally needed technologies or services and negotiate preliminary terms and conditions - Early involvement of all suppliers and/or service providers will increase the preparedness for deviations and will enable them to provide additional supplies and/or resources.

Operational Level	Response / Recovery	Service & Infrastructure operations - Keep “IT” running	**OL 1.1 Establish a service desk for incident, event and request handling** - A single point of contact for all IT related issues and requests should be established. This will reduce confusion and make tracking of incidents and solutions easier.
			OL 1.2 Prioritize incidents, events, and requests based on process impact - Critical incidents, events and request must be treated first. Hence, the impact and estimated time to solve the issue has to be used to prioritize occurring incidents.
			OL 1.3 Identify and execute emergency changes based on process impact - Emergency changes have top priority. Due to the reduced "change management" procedures they can have unforeseen impact. Hence, all involved parties and decision makers should be alarmed and prepared.
			OL 1.4 Implement effective and efficient escalation routines- Some incidents cannot be solved by the service desk, therefore escalation processes should be known to forward more difficult issues to specialists or decision makers (e.g. for emergency changes).
			OL 2.1 Use a configuration repository to collect and retrieve information about IT services and IT assets - Before changes are made consult the configuration repository to make sure that all circumstances, dependencies and configurations are known.
			OL 2.2 Document necessary changes, solutions and closures - Documented all changes, solutions and closures regarding an IT service, IT asset or IT security policy in a way that others can reproduce, undo and analyze the changes made.
			OL 3.1 Proactively maintain critical servers, networks, software and fallback systems - Critical infrastructures and services have to be pro-actively managed to minimize downtimes and/or errors and maximize availability and/or quality.
			OL 3.2 Co-maintain inter-organizational services and interfaces - When working in an inter-organizational setting maintenance of mutually used IT services and IT infrastructures has to be coordinated with all participating organizations.

Audit & Control	All / Transition & Improvement	Monitor, Control & Improve	**AC 1.1 Define key performance indicators to measure the performance of your processes and IT infrastructure** - Indicators are important to measure performance and make predictions about future developments. Standard KPI (e.g. downtime, time to recover services, etc.) can be used but also custom KPI can be important to some organizations.
			AC 1.2 Measure and assess your processes and IT infrastructure - Frequent measurements are necessary for meaningful analysis and forecasts.
			AC 1.3 Report your performance to the IT Governance board - It is important that decision makers are informed about positive and negative performance in order to make the right decision.
			AC 1.4 Implement and follow a continual improvement process - Implementing a standardized improvement process (e.g. Deming cycle) to ensure continual improvement of IT services and avoid unwanted relapse to lower quality levels.
			AC 1.5 Review incidents and events during operation to identify recurring patterns - Analyze all incidents and events to identify recurring problems and find solutions to eliminate future incidents and events.
		Change Management	**AC 2.1 Implement change standards and procedures** - Implementation of standard procedures for changes decreases failure rates an increases quality of changes.
			AC 2.2 Implement emergency change procedures- Implementation of emergency change procedures decreases response times but ensures a minimum standard of quality.
			AC 2.3 Provide guidelines for change assessment and prioritization - Change management should provide tools (e.g. tables) to assess and prioritize changes to ensure the quality of decisions made.
			AC 2.4 Test and authorize changes - Changes should be tested and authorize on a "4 eyes" basis to ensure that no unnecessary or untested changes are made which could compromise the stability of IT services or IT assets.
			AC 2.5 Release and deploy changes - Have standardized deployment procedures to ensure that all changes made are authorized and documented.

			AC 2.6 Evaluate changes made - All changes have to be evaluated after a certain amount of time to ensure that that the changes made fulfill quality requirements and have no negative effects.
			AC 2.7 Document changes and update the configuration repository - All changes have to be documented to the configuration repository to ensure that the current configurations are available in case of incidents and/or events.
	All / Regulations	Compliance & Regulations	**AC 3.1 Identify legal, regulatory, and contractual compliance requirements** - It is necessary to know all legal, regulatory and compliance requirements in order to ensure security and privacy of sensible data.
			AC 3.2 Evaluate compliance of IT supported processes and services - All IT enabled processes have to be evaluated to ensure compliance.
			AC 3.3 Improve compliance with existing regulations and pro-actively influence new regulations to optimize IT driven EM procedures - It is not only important to improve non-compliant processes but also influence future regulations. Pro-active participation in legislative procedures can ensure security and privacy, but also give EM organization to act more efficient and effective if the regulations go along with EM procedures.
	All / Projects & Collaboration	Project & Program Management	**AC 4.1 Establish a "P3" (project, programme, portfolio) mindset and approach** - New IT initiatives have to prioritized and managed. The P3 approach can help EM organizations to find interdependencies between projects and prioritize them accordingly.
			AC 4.2 Implement a project management framework to manage scope, risk and implementation - Implementation of new IT initiatives have to managed in order to stay in scope, time and cost. Frameworks such as PMBOK and SCRUM can be helpful.
		Inter-Organizational Collaboration& Service Integration	**AC 5.1 Define information exchange procedures**- To exchange information with other organizations information exchange procedures and standard interfaces have to be defined and agreed.

			AC 5.2 Define inter-organizational security procedures - Security procedure and standards need to be defined in order to give and get access to other organizations.
			AC 5.3 Establish inter-organizational IT cooperation - Inter-organizational cooperation enable quick and easy information exchange in EM situations without compromising security and integrity of exchanged data.
			AC 5.4 Provide and maintain an inter-organizational knowledge and address database for key-staff and key-functions - If key-staff and their expertise are known to cooperating organizations, decisions can be made faster and information can be provided easier.
			AC 5.5 Establish and use mutual IT standards - Mutual It standards decrease the effort for implementations reduce costs.
			AC 5.6 Consider a purchasing association with close partners - Procuring and sharing IT resources and IT services can make processes more efficient, reduce cost significantly and increase the possibility to co-source IT infrastructures.

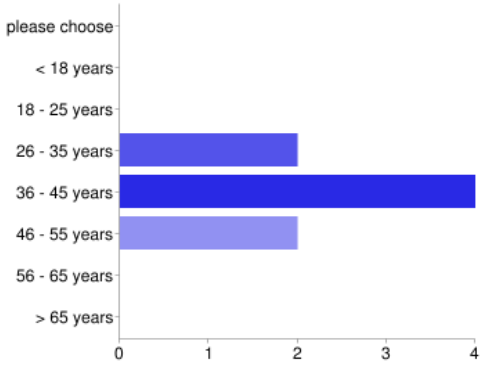
Abbreviations:	**ITICO4EM Levels**
	SL = Strategic Level
	SO = Strategic / Operational Level
	OL = Operational Level
	AC = Audit & Control Level

20 Appendix H (Evaluation Survey & Results)

Section 1: Demographic Data

This section will provide us information about your background and expertise. Please answer the question carefully. Doubtful / ambiguous submissions or submissions from participants younger than 18 years old will be deleted.

Q1: How old are you?

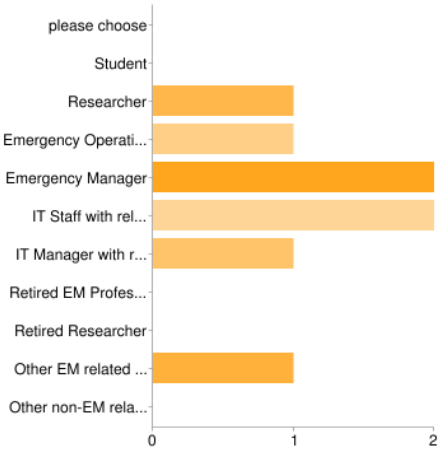


please choose	0	0%
< 18 years	0	0%
18 - 25 years	0	0%
26 - 35 years	2	25%
36 - 45 years	4	50%
46 - 55 years	2	25%
56 - 65 years	0	0%
> 65 years	0	0%

Q2: What is your country of residence?

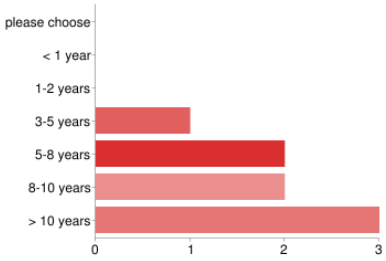
Germany Australia Hungary USA Germany USA USA Germany

Q3: What is our current occupation?



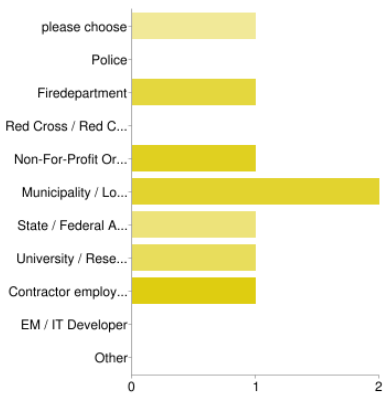
please choose	0	0%
Student	0	0%
Researcher	1	13%
Emergency Operations / First Responder	1	13%
Emergency Manager	2	25%
IT Staff with relation to EM organizations	2	25%
IT Manager with relation to EM organizations	1	13%
Retired EM Professional	0	0%
Retired Researcher	0	0%
Other EM related profession (e.g. external consultant)	1	13%
Other non-EM related profession	0	0%

Q4: How many years of experience do you have in the EM domain?



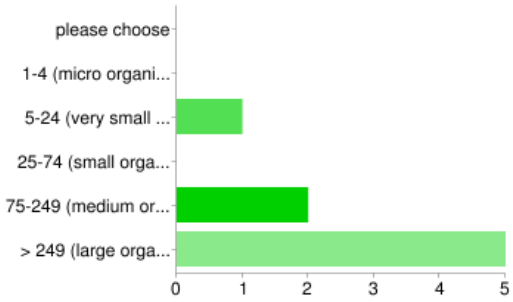
please choose	0	0%
< 1 year	0	0%
1-2 years	0	0%
3-5 years	1	13%
5-8 years	2	25%
8-10 years	2	25%
> 10 years	3	38%

Q5: What is the nature of your current organization you are working with?



please choose	1	13%
Police	0	0%
Firedepartment	1	13%
Red Cross / Red Crecent	0	0%
Non-For-Profit Organization	1	13%
Municipality / Local Government	2	25%
State / Federal Agency	1	13%
University / Research Institute	1	13%
Contractor employed by an EM orgnization (e.g. outsouced IT staff, consultant)	1	13%
EM / IT Developer	0	0%
Other	0	0%

Q6: How many people are employed in your current organization or in the EM organization you are/were working with?

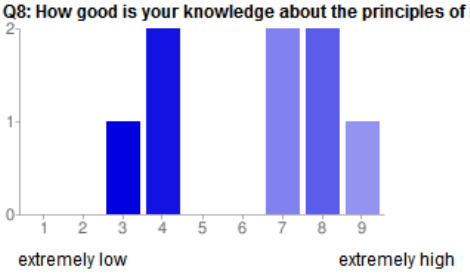


please choose	0	0%
1-4 (micro organization)	0	0%
5-24 (very small organization)	1	13%
25-74 (small organization)	0	0%
75-249 (medium organization)	2	25%
> 249 (large organization)	5	63%

Q7: How good is your expertise in IT in general?

1 - extremely low	0	0%
2	0	0%
3	0	0%
4	1	13%
5	1	13%
6	0	0%
7	1	13%
8	4	50%
9 - extremely high	1	13%

Q8: How good is your knowledge about the principles of IT Governance / IT Alignment in particular?



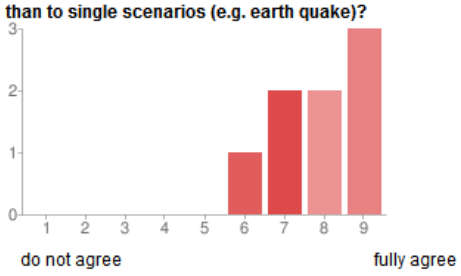
1 -	extremely low	0	0%
2		0	0%
3		1	13%
4		2	25%
5		0	0%
6		0	0%
7		2	25%
8		2	25%
9 -	extremely high	1	13%

Q9: How good is your expertise in EM procedures in general?

1 -	extremely low	0	0%
2		0	0%
3		0	0%
4		1	13%
5		2	25%
6		0	0%
7		2	25%
8		2	25%
9 -	extremely high	1	13%

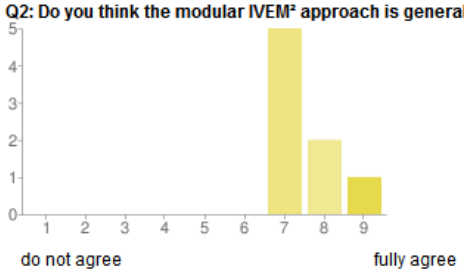
Section 2: IVEM² - IT Value Estimation Method in Emergency Management

Q1: Do you think that IT should be aligned to crucial and often re-used modules (e.g. evacuation) rather than to single scenarios (e.g. earth quake)?



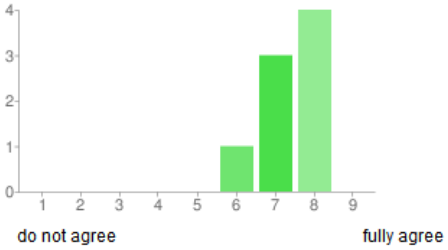
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		2	25%
8		2	25%
9 -	fully agree	3	38%

Q2: Do you think the modular IVEM² approach is generally suitable to align IT in EM organizations?



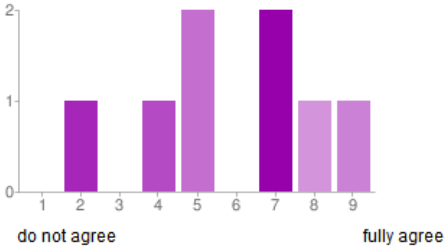
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		5	63%
8		2	25%
9 -	fully agree	1	13%

Q3: Do you think the modular IVEM² approach is flexible enough to cope with multiple/uncertain/unknown situations?



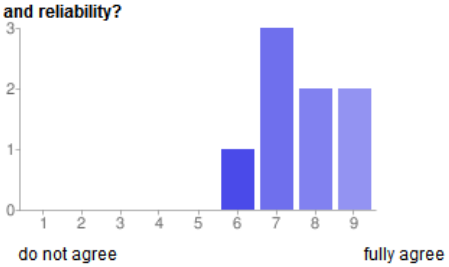
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		3	38%
8		4	50%
9 -	fully agree	0	0%

Q4: Do you think the cross-impact between IT investments / projects will be significant for an IT related decision?



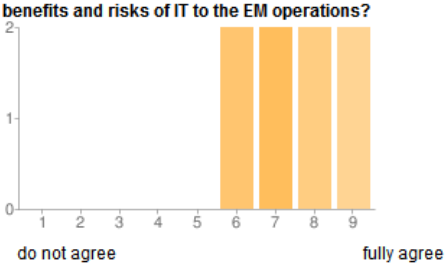
1 -	do not agree	0	0%
2		1	13%
3		0	0%
4		1	13%
5		2	25%
6		0	0%
7		2	25%
8		1	13%
9 -	fully agree	1	13%

Q5: Do you think the mapping of IT / IT Services to reusable modules will increase the IT service quality and reliability?



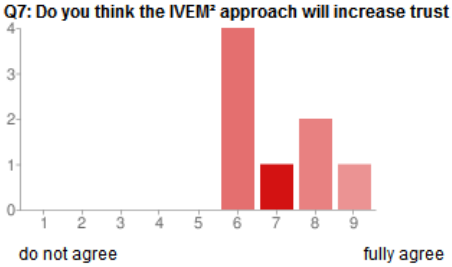
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		3	38%
8		2	25%
9 -	fully agree	2	25%

Q6: Do you think the IVEM² approach will increase transparency and increase the understanding of the benefits and risks of IT to the EM operations?



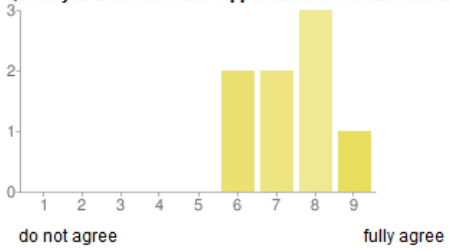
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		2	25%
7		2	25%
8		2	25%
9 -	fully agree	2	25%

Q7: Do you think the IVEM² approach will increase trust in IT enabled/supported EM processes?



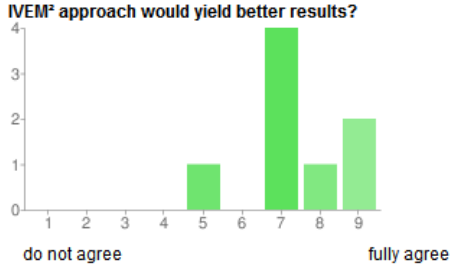
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		4	50%
7		1	13%
8		2	25%
9 -	fully agree	1	13%

Q8: Do you think the IVEM² approach will increase the utilization of IT in EM processes?



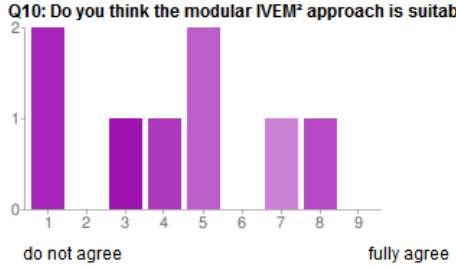
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		2	25%
7		2	25%
8		3	38%
9 -	fully agree	1	13%

Q9: If you already have an IT portfolio prioritization process in your EM organizations, do you think that the IVEM² approach would yield better results?



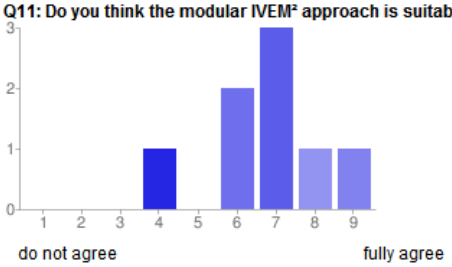
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		1	13%
6		0	0%
7		4	50%
8		1	13%
9 -	fully agree	2	25%

Q10: Do you think the modular IVEM² approach is suitable for smaller EM organizations?



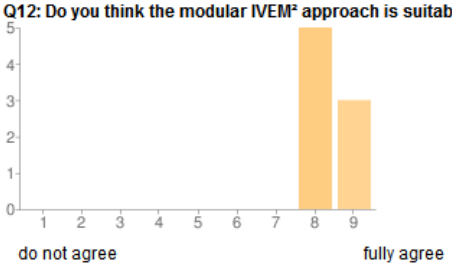
1 -	do not agree	2	25%
2		0	0%
3		1	13%
4		1	13%
5		2	25%
6		0	0%
7		1	13%
8		1	13%
9 -	fully agree	0	0%

Q11: Do you think the modular IVEM² approach is suitable for medium EM organizations?



1 -	do not agree	**0**	0%
2		**0**	0%
3		**0**	0%
4		**1**	13%
5		**0**	0%
6		**2**	25%
7		**3**	38%
8		**1**	13%
9 -	fully agree	**1**	13%

Q12: Do you think the modular IVEM² approach is suitable for large EM organizations?



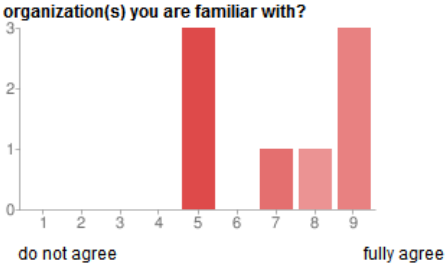
1 -	do not agree	**0**	0%
2		**0**	0%
3		**0**	0%
4		**0**	0%
5		**0**	0%
6		**0**	0%
7		**0**	0%
8		**5**	63%
9 -	fully agree	**3**	38%

Q13: If you tend NOT to agree in one or more of the above questions, please provide some feedback why you think IVEM² is not suitable to align IT in EM organizations, or where IVEM² needs some improvements.

Q9) I have not seen IVEM² in a working environment yet. In smaller EM org the relevance of technology is not yet understood and therefore also the need of ITSM / IT Governance is not yet a requirement.

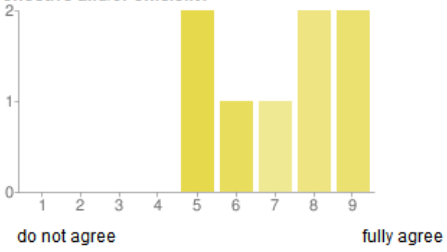
Section 3: Organizational Issues - EMIT Decision Matrix and Crisis Information Officer (CrIO)

Q1: Do you think there is a responsibility shift between the pre and post emergency phase in the EM organization(s) you are familiar with?



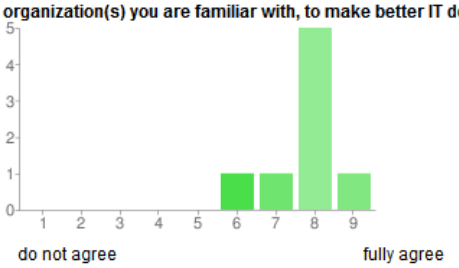
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		3	38%
6		0	0%
7		1	13%
8		1	13%
9 -	fully agree	3	38%

Q2: Do you think that such responsibility shifts can cause problems and make EM procedures less effective and/or efficient?



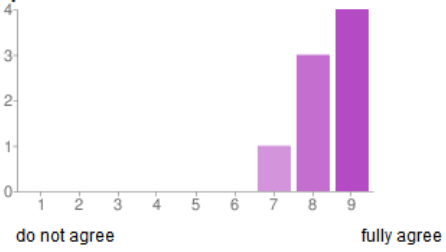
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		2	25%
6		1	13%
7		1	13%
8		2	25%
9 -	fully agree	2	25%

Q3: Do you think that the identified "to-be" pattern in the "EMIT Decision Matrix" would help EM organization(s) you are familiar with, to make better IT decisions?



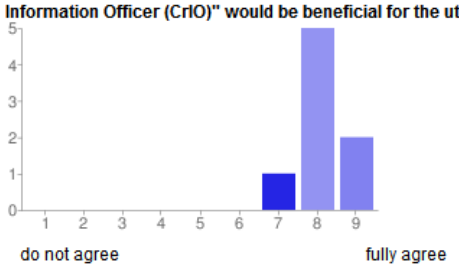
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		1	13%
8		5	63%
9 -	fully agree	1	13%

Q4: Do you think that a "Crisis Information Officer (CrIO)" would be helpful to "translate" between EM operations and IT staff?



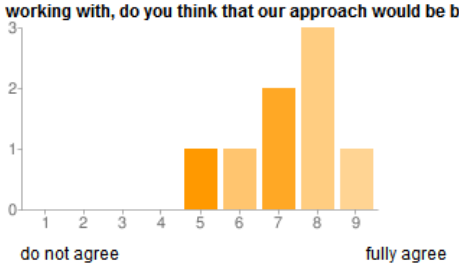
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		1	13%
8		3	38%
9 -	fully agree	4	50%

Q5: Do you think that the proposed combination of the "to-be EMIT Decision Matrix" and the "Crisis Information Officer (CrIO)" would be beneficial for the utilization of IT in EM organizations in general?



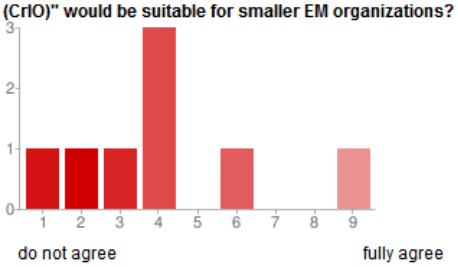
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		1	13%
8		5	63%
9 -	fully agree	2	25%

Q6: Compared to the organizational structure and IT decision making in the EM organization you are working with, do you think that our approach would be better?



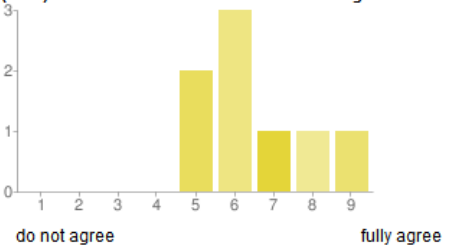
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		1	13%
6		1	13%
7		2	25%
8		3	38%
9 -	fully agree	1	13%

Q7: Do you think that combination of the "to-be EMIT Decision Matrix" and the "Crisis Information Officer (CrIO)" would be suitable for smaller EM organizations?



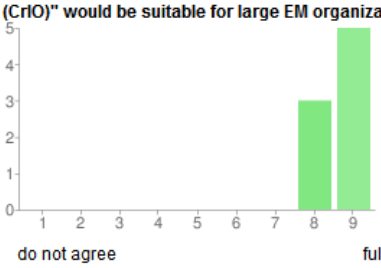
1 -	do not agree	1	13%
2		1	13%
3		1	13%
4		3	38%
5		0	0%
6		1	13%
7		0	0%
8		0	0%
9 -	fully agree	1	13%

Q8: Do you think that combination of the "to-be EMIT Decision Matrix" and the "Crisis Information Officer (CrIO)" would be suitable for medium EM organizations?



1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		2	25%
6		3	38%
7		1	13%
8		1	13%
9 -	fully agree	1	13%

Q9: Do you think that combination of the "to-be EMIT Decision Matrix" and the "Crisis Information Officer (CrIO)" would be suitable for large EM organizations?

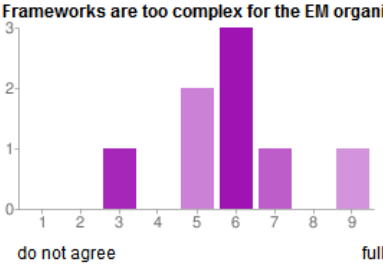


1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		0	0%
8		3	38%
9 -	fully agree	5	63%

Q10: If you tend NOT to agree in one or more of the above questions, please provide some feedback why you think these organizational changes are not suitable to EM organizations, or where they need some improvements.

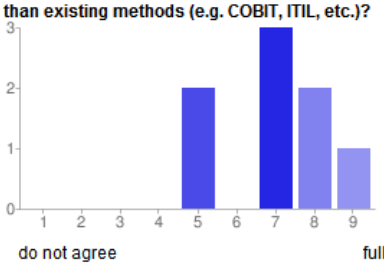
Section 4: Domain Specific Adaptation of Existing IT Governance and IT Service Management Frameworks

Q1: Do you think that existing IT Governance (e.g. COBIT) and/or IT Service Management (e.g. ITIL) Frameworks are too complex for the EM organization(s) you are familiar with?



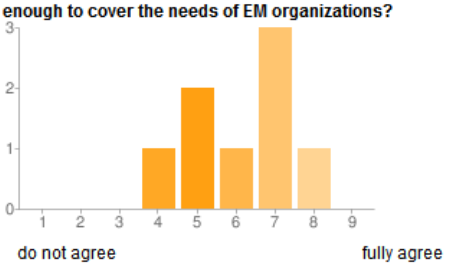
1 -	do not agree	0	0%
2		0	0%
3		1	13%
4		0	0%
5		2	25%
6		3	38%
7		1	13%
8		0	0%
9 -	fully agree	1	13%

Q2: Do you think that our conceptual and EM domain specific IT Governance framework is less complex than existing methods (e.g. COBIT, ITIL, etc.)?



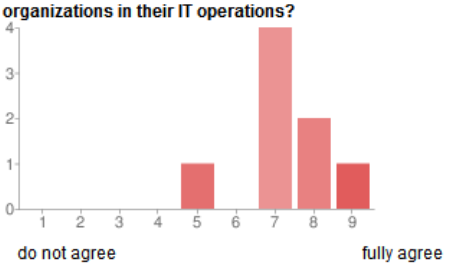
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		2	25%
6		0	0%
7		3	38%
8		2	25%
9 -	fully agree	1	13%

Q3: Do you think that our conceptual and EM domain specific IT Governance framework is detailed enough to cover the needs of EM organizations?



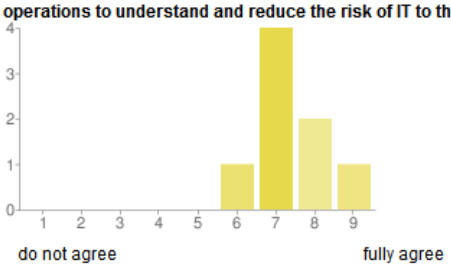
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		1	13%
5		2	25%
6		1	13%
7		3	38%
8		1	13%
9 -	fully agree	0	0%

Q4: Do you think that our conceptual and EM domain specific IT Governance framework will support EM organizations in their IT operations?



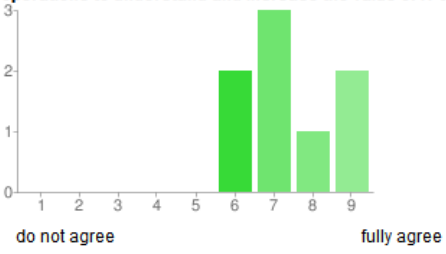
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		1	13%
6		0	0%
7		4	50%
8		2	25%
9 -	fully agree	1	13%

Q5: Do you think that our conceptual and EM domain specific IT Governance framework will help EM operations to understand and reduce the risk of IT to their operations?



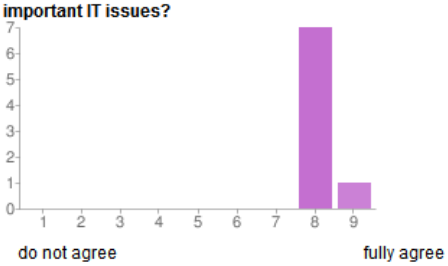
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		4	50%
8		2	25%
9 -	fully agree	1	13%

Q6: Do you think that our conceptual and EM domain specific IT Governance framework will help EM operations to understand and increase the value of IT to their operations?



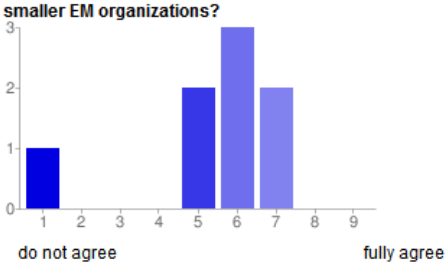
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		2	25%
7		3	38%
8		1	13%
9 -	fully agree	2	25%

Q7: Do you think that our conceptual and EM domain specific IT Governance framework have summarized and prioritized the controlled objective and best practices correctly? Does the framework cover the most important IT issues?



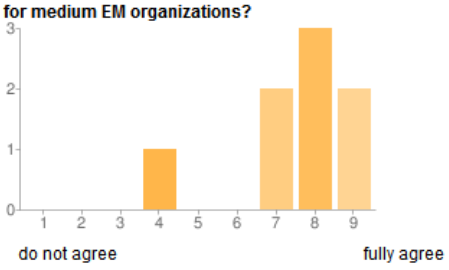
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		0	0%
8		7	88%
9 -	fully agree	1	13%

Q8: Do you think that our conceptual and EM domain specific IT Governance framework is suitable for smaller EM organizations?



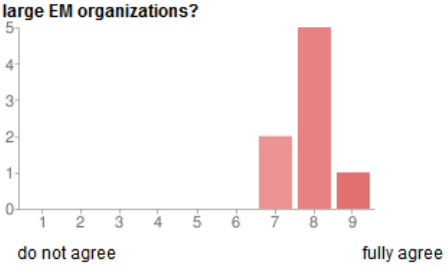
1 -	do not agree	1	13%
2		0	0%
3		0	0%
4		0	0%
5		2	25%
6		3	38%
7		2	25%
8		0	0%
9 -	fully agree	0	0%

Q9: Do you think that that our conceptual and EM domain specific IT Governance framework is suitable for medium EM organizations?



1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		1	13%
5		0	0%
6		0	0%
7		2	25%
8		3	38%
9 -	fully agree	2	25%

Q10: Do you think that our conceptual and EM domain specific IT Governance framework is suitable for large EM organizations?

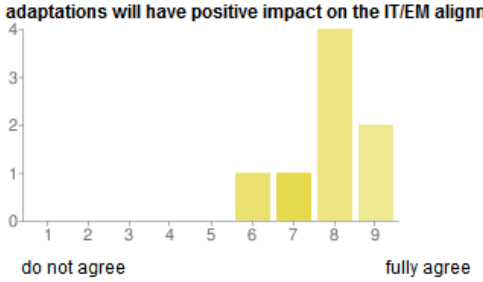


1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		2	25%
8		5	63%
9 -	fully agree	1	13%

Q11: If you tend NOT to agree in one or more of the above questions, please provide some feedback why you think these framework changes are not suitable to EM organizations, or where they need some improvements.

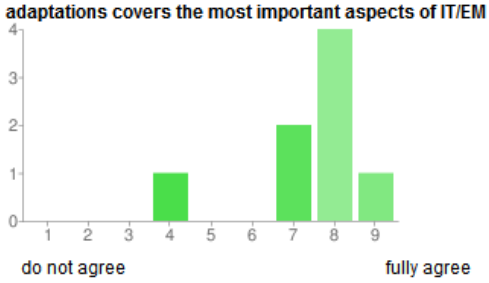
Section 5: The ITEM Reference Model as a whole

Q1: Do you think that the combination of IVEM², EMIT Decision Matrix + CrIO, and COBIT/ITIL framework adaptations will have positive impact on the IT/EM alignment?



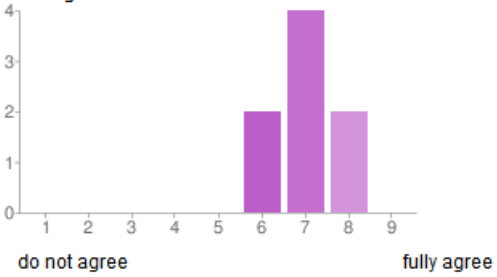
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		1	13%
7		1	13%
8		4	50%
9 -	fully agree	2	25%

Q2: Do you think that the combination of IVEM², EMIT Decision Matrix + CrIO, and COBIT/ITIL framework adaptations covers the most important aspects of IT/EM alignment?



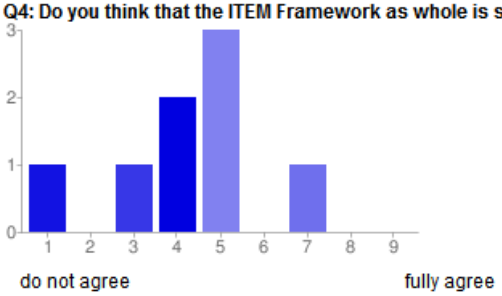
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		1	13%
5		0	0%
6		0	0%
7		2	25%
8		4	50%
9 -	fully agree	1	13%

Q3: Do you think that the ITEM Framework as whole would be suitable for the EM organization(s) you are working with?



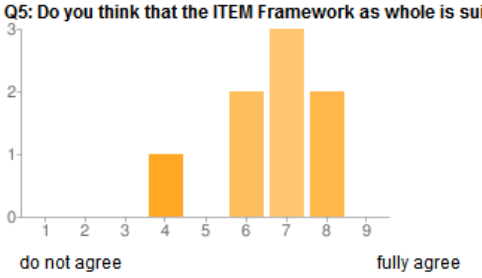
1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		2	25%
7		4	50%
8		2	25%
9 -	fully agree	0	0%

Q4: Do you think that the ITEM Framework as whole is suitable for smaller EM organizations?



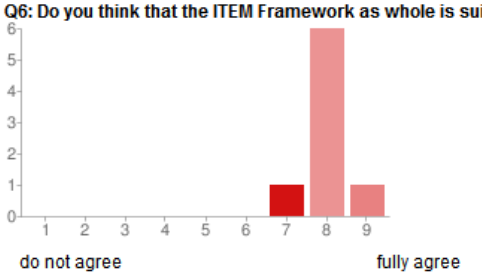
1 -	do not agree	1	13%
2		0	0%
3		1	13%
4		2	25%
5		3	38%
6		0	0%
7		1	13%
8		0	0%
9 -	fully agree	0	0%

Q5: Do you think that the ITEM Framework as whole is suitable for medium EM organizations?



1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		1	13%
5		0	0%
6		2	25%
7		3	38%
8		2	25%
9 -	fully agree	0	0%

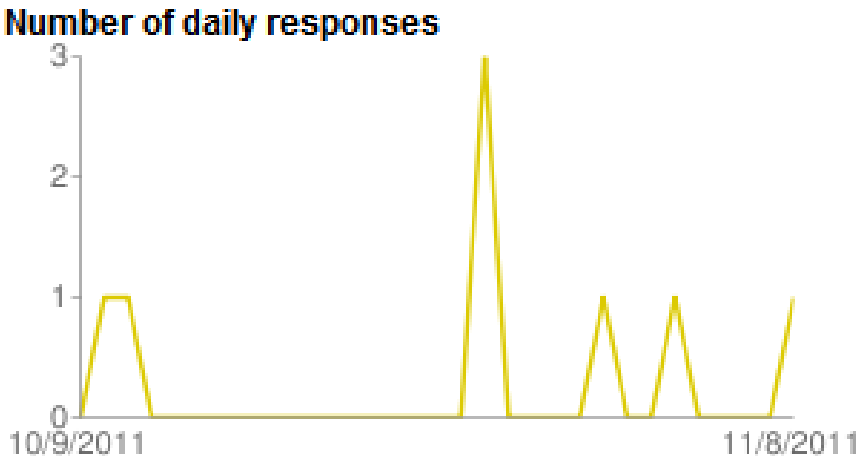
Q6: Do you think that the ITEM Framework as whole is suitable for large EM organizations?



1 -	do not agree	0	0%
2		0	0%
3		0	0%
4		0	0%
5		0	0%
6		0	0%
7		1	13%
8		6	75%
9 -	fully agree	1	13%

Q7: If you tend NOT to agree in one or more of the above questions, please provide some feedback why you think that the ITEM Framework as whole is not suitable to EM organizations, or where it needs some improvements.

Thank YOU for your valuable time!



Paste your long URL here:

Shorten http://goo.gl/...

All goo.gl URLs and click analytics are public and can be shared by anyone.

Clicks for the past: two hours | day | week | month | **all time**

Long URL	Short URL	Created	Clicks	
https://docs.google.com/leaf?id=0BxYldk63TyLXM	goo.gl/yOvZh	Oct 9, 2011	**30**	Details »
https://docs.google.com/leaf?id=0BxYldk63TyLXY	goo.gl/k3USq	Oct 9, 2011	**14**	Details »
https://docs.google.com/leaf?id=0BxYldk63TyLXO	goo.gl/U2HJH	Oct 9, 2011	**13**	Details »
https://spreadsheets.google.com/spreadsheet/viev	goo.gl/vUYvx	Aug 16, 2011	**62**	Details »

Hide URL Hidden URLs remain public, but are permanently removed from your dashboard. Page **1** of **1**

Long URL: https://spreadsheets.google.com/spreadsheet/viewform?formkey=dEJNUjYxbEN4eGNGc1ltNDZxM0NSQlE6MQ

Short URL: goo.gl/vUYvx

Created: Aug 16, 2011

Report spam

http://goo.gl/vUYvx.qr

Clicks for the past: two hours | day | week | month | **all time**

Clicks

62 clicks on this short URL

62 total clicks on all goo.gl short URLs pointing to this long URL

Traffic sources

Referrers	
Unknown/empty	49
bl157w.blu157.mail.li	9
goo.gl	2
bl132w.blu132.mail.li	1
cecid.com	1

Visitor profile

Countries	
Germany	26
United States	13
France	4
Canada	3
United Kingdom	3
Sweden	3
Australia	1
Belgium	1
Estonia	1
Greece	1

Browsers	
Internet Explorer	30
Firefox	20
Chrome	8
Opera	2
Safari	2

Platforms	
Windows	51
Macintosh	6
Other Unix	4
iPad	1

Long URL: https://docs.google.com/leaf?id=0BxYldk63TyLXMGFhNmM1YTMtM2E5Yy00NDA4LWExYmUtZTFiOGUzMjllOTM5&hl=en_US

Short URL: goo.gl/yOvZh

Created: Oct 9, 2011

Report spam

http://goo.gl/yOvZh.qr

Clicks for the past: two hours | day | week | month | **all time**

Clicks

30 clicks on this short URL

30 total clicks on all goo.gl short URLs pointing to this long URL

Traffic sources

Referrers	
Unknown/empty	26
spreadsheets.google	3
goo.gl	1

Visitor profile

Countries	
Germany	11
United States	10
Australia	2
France	2
Belgium	1
United Kingdom	1
Hungary	1
Netherlands	1
Norway	1

Browsers	
Internet Explorer	15
Firefox	9
Chrome	5
Safari	1

Platforms	
Windows	25
Macintosh	3
Other Unix	1
iPad	1

Long URL: https://docs.google.com/leaf?id=0BxYldk63TyLXYjQ5NTU1ZjgtYjg2ZC00N2FlLWI2ODItYWU3MzdiY2M3NzQ2&hl=en_US

Short URL: goo.gl/k3USq

Created: Oct 9, 2011

Report spam

http://goo.gl/k3USq.qr

Clicks for the past: two hours | day | week | month | **all time**

Clicks

14 clicks on this short URL

14 total clicks on all goo.gl short URLs pointing to this long URL

Traffic sources

Referrers	
Unknown/empty	10
spreadsheets.google	3
goo.gl	1

Visitor profile

Countries	
United States	7
Australia	2
Germany	2
France	1
United Kingdom	1
Hungary	1

Browsers	
Internet Explorer	7
Chrome	5
Firefox	2

Platforms	
Windows	13
Macintosh	1

Long URL: https://docs.google.com/leaf?id=0BxYldk63TyLXODZlODRjMmYtZDg3MS00NmUzLTg2NjQtYzI3NTZjNzM2YTUx&hl=en_US

Short URL: goo.gl/U2HJH

Created: Oct 9, 2011

Report spam

http://goo.gl/U2HJH.qr

Clicks for the past: two hours | day | week | month | **all time**

Clicks

13 clicks on this short URL

13 total clicks on all goo.gl short URLs pointing to this long URL

Traffic sources

Referrers	
Unknown/empty	9
spreadsheets.google	3
goo.gl	1

Visitor profile

Countries	
United States	7
Germany	2
Australia	1
France	1
United Kingdom	1
Hungary	1

Browsers	
Internet Explorer	6
Chrome	5
Firefox	2

Platforms	
Windows	12
Macintosh	1

21 Bibliography

Achtenhagen, L., Melin, L., Müllern, T., & Ericson, T. (2003). The Role of Interactive strategizing. In A. M. Pettigrew, R. Whittington, L. Melin, C. Sanchez-Runde, F. A. J. Van den Bosch, W. Ruigrok & T. Numagami (Eds.), *Innovative Forms of Organizing: International Perspectives*: Sage Publications Ltd.

Addy, R. (2007). *Effective IT Service Management: To ITIL and Beyond*. Berlin: Springer.

Andrade, A. D. (2009). Interpretive Research Aiming at Theory Building: Adopting and Adapting the Case Study Design *The Qualitative Report, 14*(1), 42-60.

Arbnor, I., & Bjerke, B. (2009). *Methodology for Creating Business Knowledge, 3rd edt.*: SAGE Publishing.

Bandayrel, K., Lapinsky, S., & Christian, M. (2011). Information Technology Systems for Critical Care Triage and Medical Response During an Influenza Pandemic: A Review of Current Systems. *Disaster Medicine and Public Health Preparedness*, dmp.2011.2045.

Barton, L. (2007). *Leadership now: A real-world guide to preparing for threats, disaster, sabotage, and scandal*. New York, USA: McGraw-Hill.

Baskerville, R. L., & Wood-Harper, A. T. (1996). A Critical Perspective on Action Research as a Method for Information Systems Research. *Journal of Information Technology, 11*, 235-246.

Baskerville, R. L., & Wood-Harper, A. T. (1998). Diversity in information systems action research methods. *European Journal of Information Systems, 7*, 90-107.

Becker, J., Dreiling, A., & Ribbert, M. (2002). *Contribution of Meta-models to Systems Engineering: A CRM Example.* Paper presented at the Information Systems Foundation: Building the Theoretical Base, Canberra, ACT, Australia.

Becker, J., Dreiling, A., & Ribbert, M. (2003). *Meta Model based Approaches to Information Systems Engineering.* Paper presented at the Information Resources Management Association Conference, Philapelphia, PA, USA.

Becker, J., Knackstedt, R., Pfeiffer, D., & Janiesch, C. (2007). *Configurative Method Engineering - On the Applicability of Reference Modeling Mechanisms in Method Engineering.* Paper presented at the Americas Conference on Information Systems (AMCIS), Keystone, CO, USA.

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in IS: The Practice of Relevance. *MIS Quarterly, 23*(1), 3-16.

Berelson, B. (1952). *Content analysis in communicatin research*. Glence Ill., USA: Free Press.

Berthon, P., Pitt, L., Ewing, M., & Carr, C. L. (2002). Potential Research Space in MIS: A Framework for Envisioning and Evaluating Research Replication, Extension, and Generation. *Information Systems Research, 13*(4), 416-427.

Bhattacharjya, J., & Chang, V. (2007). Evolving IT Governance Practices for Aligning IT with Business - A Case Study in an Australian Institution of Higher Education. *Journal of Information Science and Technology (JIST), 4*(1), 24-46.

Bjorner, D. (2010). Domain Engineering. In P. Boca, J. P. Bowen & J. Siddiqi (Eds.), *Formal Methods: State of the Art and New Directions* (pp. 1-41): Springer London.

Bleicher, J. (1980). *Contemporary hermeneutics: hermeneutics as method, philosophy, and critique*. Oakland, CA, USA: Routledge & Kegan Paul.

Boland, R. J. (1985). Phenomenology: A Preferred Approach to Research in Information Systems. In E. Mumford, R. Hirschheim, G. Fitzgerald & A. T. Wood-Harper (Eds.), *Research Methods in Information Systems* (pp. 193-201). Amsterdam, Netherlands: North Holland.

Borodzicz, E. P. (2005). *Risk, crisis and security management*. West Sussex, England: John Wiley & Sons.

Böttcher, R. (2008). *IT-Servicemanagement mit ITIL V3*. Hannover: Heise Verlag.

Brennan, J. A., & Krohmer, J. R. (2005). *Principles of EMS systems*. Sudbury, MA, USA: Jones & Bartlett Publishers.

Brenner, M., Garschhammer, M., & Hegering, H.-G. (2006). When Infrastructure Management Just Won't Do: The Trend Towards Organizational IT Service Management. In E.-M. Kern, H.-G. Hegering & B. Brügge (Eds.), *Managing Development and Application of Digital Technologies* (pp. 131-146): Springer Berlin Heidelberg.

Brownstein, J. S., Freifeld, C. C., Chan, E. H., Keller, M., Sonricker, A. L., Mekaru, S. R., et al. (2010). Information Technology and Global Surveillance of Cases of 2009 H1N1 Influenza. *New England Journal of Medicine, 362*(18), 1731-1735.

Bundesministerium des Inneren, B. M. I. (2008). *Krisenkommunikation, Leitfaden für Behörden und Unternehmen*.

Calder, A., & Moir, S. (2009). The Calder-Moir IT Governance Framework Retrieved May 06, 2009, from http://www.itgovernance.co.uk/calder_moir.aspx

Cavana, R., Delahaye, B. L., & Sekeran, U. (2001). *Applied Business research: Qualitative and Quantitative Methods*. Milton, QLD, Australia: John Wiley & Sons Australia.

Chaczko, Z., & Ahmad, F. (2005). *Wireless Sensor Network Based System for Fire Endangered Areas.* Paper presented at the Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05) Volume 2 - Volume 02.

Chan, T., Fielt, E., Gable, G. G., & Stark, K. (2010). Smart Services CRC - Service and Service Quality *Business Service Management, Volume 2,* 46.

Chan, Y. E. (2000). IT Value: The Great Divide Between Qualitative and Quantitative and Individual and Organizational Measures. [Article]. *Journal of Management Information Systems, 16*(4), 225-261.

Chan, Y. E. (2002). Why Haven't We Mastered Alignment? The Importance of the Informal Organization Structure. *MIS Quarterly Executive, 1*(2), 97 - 112.

Chase, R. B., Jacobs, F. R., & Aquilano, N. J. (2006). *Operations Management for Competitive Advantage (11th ed.)*. Boston, USA: McGraw-Hill.

Chase, S. E. (2003). Learning to listen: narrative principles in a qualitative research methods course. In R. Josselson, A. Lieblich & D. P. McAdams (Eds.), *Up Close and Personal: The Teaching and Learning of Narrative Research* (pp. 79-100). Washington, DC, USA: American Psychological Association.

Chorafas, D. (2004). *Operational risk control with Basel II: Basic principles and capital requirements*. Oxford, UK: Elsevier Butterworth-Heinemann.

Chua, W. F. (1986). Radical Developments in Accounting Thought - A critique and overview of the development of interpretive research in accounting. *The Accounting Review, 61*, 601-632.

Cole, M., & Avison, D. (2007). The potential of hermeneutics in information systems research. *European Journal of Information Systems, 16*, 820-833.

Costello, P. J. M. (2003). *Action Research*. London: Continuum.

Davenport, T. H., & Markus, M. L. (1999). Rigor vs. Relevance Revisited: Response to Benbasat and Zmud. *MIS Quarterly, 23*(1), 19-23.

Debreceny, R., S. (2006). *Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls.* Paper presented at the Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Department of Homeland Security (DHS), O. o. I. G. (2005). Emergency preparedness and response could better integrate information technology with incident response and recovery. Retrieved July 28, 2009, from http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_05-36_Sep05.pdf

Di Maio, A. (2003a). Traditional ROI Measures Will Fail in Government Gartner Research.

Di Maio, A. (2003b). Value for money is not enough in public sector IT projects. Gartner Research.

Di Maio, A. (2007). Worldwide Examples of Public-Value-of-IT Frameworks. Gartner Research.

Dilmaghani, R. B., & Rao, R. R. (2009). *A Systematic Approach to Improve Communication for Emergency Response.* Paper presented at the

Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Duffy, J. (2002). IT/Business alignment: Is it an option or is it mandatory? IDC.

Dunn, K. (2000). Interviewing. In I. Hay (Ed.), *Qualitative Research Methods in Human Geography* (pp. 50-81). Oxford, UK: Oxford University Press.

Dwarkanath, S., & Dakonta, M. (2006). *Emergency Services Enterprise Framework: A Service-Oriented Approach* Paper presented at the Proceedings of the 3rd International ISCRAM Conference, Newark, NJ (USA).

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review, 14*(4), 532-550.

Elsässer, W. (2005). *ITIL einführen und umsetzen: Leitfaden für effizientes IT-Management durch Prozessorientierung*. Munich: Carl Hanser Verlag.

Emergency Management Queensland (EMQ), Q. G. (2009). Emergency Management Queensland - Services. Retrieved August 08, 2009, from http://www.emergency.qld.gov.au/emq/

European Union (EU), E. C. J. a. H. A. (2009). Data Protection. Retrieved June 14, 2009, from http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Fettke, P., Loos, P., & Zwicker, J. (2005). *Business Process Reference Models: Survey and Classification.* Paper presented at the Third International Conference on Business Process Management (BPM), Nancy, France.

Fischer, S. (2002). *Basel II: Risk Management and Implications for Banking in Emerging Market Countries.* Paper presented at the International Conference of Banking Supervisors, Cape Town, South Afrika.

Flick, U. (2002). *An introduction to qualitative research*: Sage Publications Ltd.

FLOODsite, & SOGREAH. (2009). FOODsite Project, European Community's Sixth Framework Programme, Task 17 & 19. Retrieved September 09, 2009, from http://www.floodsite.net/html/cd_task17-19/flood_management_practice.html

Frank, U. (1999). *Conceptual Modelling as the Core of the Information Systems Discipline - Perspectives and Epistemological Challenges.* Paper presented at the 5th America's Conference on Information Systems (AMCIS 99), Milwaukee, USA.

Frank, U. (2000). Modelle als Evaluationsobjekt: Einführung und Grundlegung. In I. Häntschel & L. J. Heinrich (Eds.), *Evaluation und Evaluationsforschung in der Wirtschaftsinformatik* (pp. 339-352). München, Germany: Oldenbourg Verlag.

Frank, U. (2003). Für Sie gelesen: IS Research Relevance Revisited: Subtle Accomplishment, Unfulfilled Promise, or Serial Hypocrisy? *Wirtschaftsinformatik, 43*(3), 354-357.

Frank, U. (2007). Evaluation of Reference Models. In P. Fettke & P. Loos (Eds.), *Reference Modeling for Business Systems Analysis* New York, USA: Idea Group Inc. / IGI Global.

Fridriksson, H. V. (2008). *Learning processes in an inter-organizational context.* Unpublished Dissertation, Jönköping International Business School, Jönköping, Sweden.

Fry, M. (2010). *ITIL Lite: A Road Map to Full or Partial ITIL Implementation*. London, UK: The Stationery Office.

Fry, M. (2011). How to Implement a Lite Version of ITIL® v3. Retrieved July 11, 2011, from http://www.hthts.com/Teleseminars/Malcolmfry.pdf

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems, 3*(2), 112-126.

Ghauri, P. N., & Gronhaug, K. (2005). *Research methods in business studies: a practical guide, 3rd Edt.* New York, NY, USA: Financial Times Prentice Hall.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, Illinois, USA: Aldine Publ.

Goeken, M., & Alter, S. (2008). *Representing IT Governance Frameworks as Metamodels.* Paper presented at the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'08), World Congress in Computer Science (Worldcomp'08), Las Vegas, Nevada, USA.

Goeken, M., & Alter, S. (2009). *Towards Conceptual Metamodeling of IT Governance Frameworks Approach - Use - Benefits.* Paper presented at the 42nd Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, USA.

Goeken, M., Alter, S., Milicevic, D., & Patas, J. (2009). Metamodelle von Referenzmodellen am Beispiel ITIL: Vorgehen, Nutzen, Anwendung. *Lecture Notes in Informatics (LNI), P-154*, 473-481.

Gorman, G. E., Clayton, P., Shep, S. J., & Clayton, A. (2005). *Qualitative Research For The Information Professional: A Practical Handbook (2nd edt)*: Neal-Schuman Publishers.

Guba, E. G., & Lincoln, Y. S. (1994). Competing Paradigms in Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 105-117). Thousand Oaks, CA, USA: Sage Publications.

Guha-Sapir, D., & Lechat, M. F. (1986). Information systems and needs assessment in natural disasters: An approach for better disaster relief management. *Disasters, 10*(3), 232-237.

Guldentops, E. (2003). Governing Information Technology through COBIT. In W. Van Grembergen (Ed.), *Strategies for information technology governance* (pp. 269 - 309). Hershey, Pa.: Idea Group Publishing.

Harrald, J. R. (2006). Agility and Discipline: Critical Success Factors for Disaster Response. *The ANNALS of the American Academy of Political and Social Science, 604*(1), 256-272.

Harrald, J. R. (2011). Achieving Agility in Disaster Management. *International Journal of Information Systems for Crisis Response and Management, 1*(1), 1-11.

Hedin, G., Ohlsson, L., & McKenna, J. (1998). Product configuration using object oriented grammars. In B. Magnusson (Ed.), (Vol. 1439, pp. 107-126): Birkhäuser Basel.

Heinrich, L., & Sinz, E. (2002). Wirtschaftsinformatik. In P. Rechenberg & G. Pomberger (Eds.), *Informatik-Handbuch*. Munich, Germany: Hanser Verlag.

Held, D. (1980). *Introduction to Critical Theory: Horkheimer to Habermas*. Berkley, CA, USA: University of California Press.

Henderson, J., & Venkatraman, N. (1992). *Strategic alignment: a model for organizational transformation via information technology*: Oxford University Press, USA.

Hirschheim, R. (1992). Information Systems Epistemology: An Historical Perspective. In R. Galliers (Ed.), *Information Systems Research: Issues, Methods and Practical Guidelines*. Oxford, UK: Blackwell Scientific Publications.

Hirschheim, R., & Klein, H. (1994). Realizing Emancipatory Principles in Information Systems Development: The Case for ETHICS. *MIS Quarterly, 18*(1), 83-109.

IAEM, I. A. o. E. M. (2009). Principles of Emergency Management. Retrieved August 13, 2009, from http://www.iaem.com/EMPrinciples/documents/PrinciplesOfEmergencyManagement.pdf

Iannella, R., & Henricksen, K. (2007). *Managing Information in the Disaster Coordination Centre: Lessons and Opportunities.* Paper presented at the Proceedings of the 4th International ISCRAM Conference, Delft, Netherlands.

Iannella, R., Robinson, K., & Rinta-Koski, O.-P. (2007). *Towards a Framework for Crisis Information Management Systems.* Paper presented at the 14th Annual Conference of The International Emergency Management Society (TIEMS), Trogir, Croatia.

IET-Solutions, I. E. T. (2008). ITIL Life-Cycle. Retrieved April 05, 2008, from http://www.iet-solutions.com/images/solutions/itsm-v3.gif

IFRC&RCS, I. F. o. R. C. a. R. C. (1998). *World Disaster Report 1998 - Urban Disasters*. Geneva, Switzerland: International Federation of Red Cross and Red Crescent Societies.

IT Governance Institute, I. T. G. I. (2003). Board Briefing on IT Governance, 2nd Edition. Retrieved November 15, 2008, from http://www.isaca.org/Knowledge-Center/Research/Documents/BoardBriefing/26904_Board_Briefing_final.pdf

IT Governance Institute, I. T. G. I. (2006a). Enterprise Value. Governance of IT Investments, The Val IT Framework. Retrieved August 14, 2009, from http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

IT Governance Institute, I. T. G. I. (2006b). Enterprise Value: Governance of IT Investments, The Business Case. Retrieved August 14, 2009, from http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/VAL-IT-business-case.pdf

IT Governance Institute, I. T. G. I. (2006c). Enterprise Value: Governance of IT Investments, The ING Case Study. Retrieved May 22, 2009, from http://itu.dk/people/petermeldgaard/Hovedopgave/itg/IT-Governance%20Speciale/Litterature/ITGI%20-%20The%20ING%20Case%20Study.pdf

IT Governance Institute, I. T. G. I. (2007a). COBIT Quickstart, 2nd Edition. Retrieved May 22, 2009, from http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT_Quickstart_2ndEd_15Oct07_Research.pdf

IT Governance Institute, I. T. G. I. (2007b). Control Objectives for Information and Related Technology, Version 4.1. Retrieved May 22, 2009, from http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf

IT Governance Institute, I. T. G. I. (2007c). VAL IT Case Study: Value Governance - The Police Case Study. Retrieved May 22, 2009, from http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Value-Governance-Police-Case-Study.pdf

IT Governance Institute, I. T. G. I. (2008a). Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. Retrieved May 22, 2009, from http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf

IT Governance Institute, I. T. G. I. (2008b). COBIT Mapping: Mapping of ITIL v3 With COBIT®4.1. Retrieved May 22, 2009, from http://miha.ef.uni-lj.si/_dokumenti3plus2/196062/ITIL-COBIT.pdf

IT Governance Institute, I. T. G. I. (2008c). Enterprise Value: Governance of IT Investments,The Val IT Framework 2.0 Extract. Retrieved May 22, 2009, from http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Framework-2.0-Extract-Jul-2008.pdf

IT Governance Institute, I. T. G. I. (2010a). COBIT® 5 Design Paper Exposure Draft. Retrieved December 22, 2010, from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT5_Design_Exposure_18Mar2010.pdf

IT Governance Institute, I. T. G. I. (2010b). Risk IT - Brochure. Retrieved January 20, 2011, from http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Documents/Risk-IT-Brochure.pdf

IT Service Management Forum, I. T. S. M. F. (2008). *ITIL-COBIT-Mapping: Gemeinsamkeiten und Unterschiede der IT-Standards*: Symposion Publishing.

IT Service Management Forum, I. T. S. M. F. (2009a). Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit: Management Summary Retrieved February 06, 2011, from http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf

IT Service Management Forum, I. T. S. M. F. (2009b). Source of Best Practice. Retrieved August 14, 2009, from http://www.itsmf.co.uk/BestPractice/Source_Best_Practice.aspx

Jackson, M. A. (1975). *Principles of Program Design*. Orlando, FL, USA: Academic Press, Inc.

Jacoby, R. (2009). Communicating IT's Value. [Article]. *CIO Insight*(110), 20-20.

Jayaratna, N. (1994). *Understanding and Evaluating Methodologies: NIMSAD, a Systematic Framework*. New York, NY, USA: McGraw-Hill.

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. [Article]. *MIS Quarterly, 12*(4), 571-586.

Kaplan, B., & Maxwell, J. A. (1994). Qualitative Research Methods for Evaluating Computer Information Systems. In J. G. Anderson, C. E. Aydin & S. J. Jay (Eds.), *Evaluating Health Care Information Systems: Methods and Applications* (pp. 45-68). Thousans Oaks, CA, USA: Sage Publishing.

Karagiannis, D. (1995). BPMS: business process management systems. *SIGOIS Bulletin, 16*(1), 10-13.

Karagiannis, D., & Hoefferer, P. (2006). *Metamodels in action: An overview.* Paper presented at the International Conference on Software and Data Technologies (ICSOFT), Setubal, Portugal.

Karagiannis, D., & Kühn, H. (2002). *Metamodelling Platforms.* Paper presented at the Third International Conference on E-Commerce and Web Technologies (EC-WEB 2002), Aix-en-Provence, France.

Kempter, S., & Kempter, A. (2009). Einführung: ISO 20000 und die ITIL - ISO 20000 Bridge. Retrieved August 14, 2009, from http://de.it-processmaps.com/media/einfuehrung_itil_iso_20000_bridge.pdf

Kerlinger, F., & Lee, H. (1999). *Foundations of Behavioral Research, 4th Edt.* Belmont, CA, USA: Wadsworth Publishing.

Kerr, K. (2003). Putting cyberterrorism into context. *AusCERT Member Newsletter, 7*(2).

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly Executive, 23*(1), 67-93.

Krcmar, H. (1998). *Einige Überlegungen zu Methoden der empirischen Forschung in der Wirtschaftsinformatik.* Paper presented at the

Arbeitstagung Wissenschaftstheorie in der Wirtschaftsinformatik, Universität Münster.

Küller, P., Vogt, M., Hertweck, D., & Grabowski, M. (2011). *A Domain Specific IT Service Management Approach for Small & Medium Enterprises.* Paper presented at the Proceedings of the 16th IBIMA conference on Innoviation and Knowledge Management Kuala Lumpur, Malaysia.

Kvale, S. (1996). *InterViews: An Introduction to Qualitative Research Interviewing*: SAGE Publishing.

Larsen, M. H., Pedersen, M. K., & Andersen, K. V. (2006). *IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S.* Paper presented at the 39th Annual Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii

Lee, A. S. (1999). Rigor and Relevance in MIS Research: Beyond the Approach of Positivism Alone. *MIS Quarterly, 23*(1), 29 - 34.

Leimeister, S. (2010). *IT Outsourcing Governance: Client Types and Their Management Strategies* Wiesbaden, Germany: Gabler Verlag.

Lewin, K. (1946). Action research and minority problems. *Journal of Social Issues, 2*(4), 34-46.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 22*(140), 1-55.

List, D. (2007). *Know Your Audience: A Practical Guide to Media Research, 3rd Edition*. Wellington, New Zealand: Original Books.

Looso, S., & Goeken, M. (2010). *Application of Best-Practice Reference Models of IT Governance.* Paper presented at the Proceedings of 18th European Conference on Information Systems (ECIS), Pretoria, South Africa.

Luftman, J. (2003). *Competing in the Information Age : Align in the Sand*: Oxford University Press, USA.

Luftman, J. (2004). Assessing Business-IT Alignment Maturity. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA, USA: Idea Group Publishing.

Luftman, J., & Ben-Zvi, T. (2010). Key Issues For IT Executives 2010: Judicious IT Investments Continue Post-Recession. *MIS Quarterly Executive, 9*(4), 263-273.

Luftman, J., & Kempaiah, R. (2007). An Update on Business-IT Alignment: "A Line Has Been Drawn". *MIS Quarterly Executive, 6*(3), 165-177.

Marich, M. J., Horan, T. A., & Schooley, B. L. (2008). *Understanding IT Governance within the San Mateo County Emergency Medical Service Agency.* Paper presented at the Proceedings of the 5th International ISCRAM Conference, Washington, DC, USA.

Marrone, M., & Kolbe, L. M. (2010). Uncovering ITIL claims: IT executives' perception on benefits and Business-IT alignment. *Information Systems and E-Business Management*, 1-18.

Marrone, M., & Kolbe, L. M. (2011). Impact of IT Service Management Frameworks on the IT Organization. *Business & Information Systems Engineering, 3*.

Mayring, P. (2000). *Qualitative Inhaltsanalyse. Grundfragen und Techniken.* Weinheim, Germany: Deutscher Studien Verlag.

Mayring, P. (2002). *Einführung in die Qualitative Sozialforschung*. Bale, Swizerland: Belz Verlag.

Mintzberg, H. (1979). An Emerging Strategy of "Direct" Research. *Administrative Science Quarterly, 24*(4), 582-589.

Myers, M. D. (1997). Qualitative Research in Information Systems. [Article]. *MIS Quarterly, 21*(2), 241-242.

Myers, M. D. (1999). Investigating information systems with ethnographic research. *Communications of the AIS, 2*(4), 1-20.

Myers, M. D. (2008). Qualitative Research in Information Systems, updated version. *MIS Quarterly* Retrieved June 24, 2009, from http://www.qual.auckland.ac.nz/

Mylopoulos, J., & Levesque, H. J. (1980). *An Overview of Knowledge Representation.* Paper presented at the Proceedings of the 1980 workshop On Conceptual Modelling. Perspectives from Artificial Intelligence, Databases and Programming, Pingeree Park, Col, USA.

Naumann, S. (2007). *Referenzmodellierung nicht-professioneller Domänen*. Saarbrücken, Germany: VDM Verlag Dr. Müller.

Office of Public Sector Information (OPSI), L. U. A. (1998). Data Protection Act 1998. Retrieved June 14, 2009, from http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research, 2*(1), 1-28.

Ortmann, G., Windeler, A., Becker, A., & Schulz, H. J. (1990). *Computer und Macht in Organisationen. Mikropolitische Analysen*. Opladen, Germany: Westdeutscher Verlag.

Otto, B. (2010). *IT Governance and Organizational Transformation: Findings From an Action Research Study.* Paper presented at the 16th Americas Conference on Infomation Systems (AMCIS 2010), Lima, Peru.

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., et al. (2010). *A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters.* Paper presented at the Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference, Edinburgh, United Kingdom.

Patton, M. Q. (2002). *Qualitative research and evaluation methods, 3rd Edition*. Thousand Oaks, CA, USA: Sage Publications.

Peterson, R. (2003). Information Strategies and Tactics for Information Technology Governance. In W. Van Grembergen (Ed.), *Strategies for*

information technology governance (pp. 37 - 80). Hershey, Pa.: Idea Group Publishing.

Pickard, A., & Dixon, P. (2004). The applicability of constructivist user studies: how can constructivist inquiry inform service providers and systems designers? *Information Research (IR), 9*(3), paper 175.

Popper, K. R. (1980). Science: Conjectures and Refutations. In H. Morick (Ed.), *Challenges to Empiricism* (pp. 128 - 160). London, UK: Methuen.

Porter, M. (2008). *On Competition, Updated and Expanded Edition*: Harvard Business School Press.

Project Management Institute, P. M. I. (2008). *A Guide to the Project Management Body of Knowledge (4th Edt.)*. Newtown Square, PA, USA: Project Management Inst.

QSR International, L. (2010). NVIVO 8. Doncaster, VIC, Australia.

Rao, R. R., Eisenberg, J., & Schmitt, T. (2007). *Improving Disaster Management : The Role of IT in Mitigation, Preparedness, Response, and Recovery*. Washington, DC, USA: National Academies Press.

Rapoport, R. N. (1970). Three Dilemmas in Action Research. *Human Relations, 23*(6), 499-513.

Recker, J. C. (2005). *Conceptual model evaluation. Towards more paradigmatic rigor.* Paper presented at the CAiSE'05 Workshops, Porto, Portugal.

Ridley, G., Young, J., & Carroll, P. (2004). *COBIT and Its Utilization: A Framework from the Literature.* Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS) Big Island, Hawaii.

Rijpma, J. (1997). Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory. *Journal of Contingencies and Crisis Management, 5*(1), 15-23.

Roberts, K. (1990). Managing High Reliability Organizations. *California Management Review, 27*(Summer), 101-113.

Rolf, A. (1998). *Grundlagen der Organisations- und Wirtschaftsinformatik*. Berlin, Germany: Springer.

Rolland, C. (1993). *Modeling the Requirements Engineering Process.* Paper presented at the 3rd European-Japanese Seminar on Information Modelling and Knowledge Bases Budapest, Hungary.

Routio, P. (2007). Metodi. Retrieved November 13, 2009, from http://www2.uiah.fi/projekti/metodi/eherm.gif

Rydberg Fahraeus, E. (2009). The "hermeneutic spiral" (inspired by Alvesson & Sköldberg, 1994, p. 174). Retrieved March 28, 2009, from http://people.dsv.su.se/~evafaahr/lic/lic02.gif

Saaty, T. L. (1987). Rank Generation, Preservation, anf Reversal in the Analytic Hierarchy Decision Process. *Decision Sciences, 18*(2), 157-177.

Saaty, T. L. (1990). The Analytical Hierarchy Process (AHP): How to make a decision. *European Journal of Operational Research*(48).

Salle, M. (2004). IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing. Unpublished research paper. HP Research Labs.

Salle, M., & Rosenthal, S. (2005). *Formulating and Implementing an HP IT Program Strategy using CobiT and HP ITSM.* Paper presented at the Proceeding of the 38th Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Schultze, U., & Leidner, D. (2002). Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions. *MIS Quarterly, 26*(3), 213 - 242.

Schütze, F. (1987). Das narrative Interview in Interaktionsfeldstudien, *Studienbrief der Fernuniversität Hagen*. Hagen, Germany.

Schwabe, G. (2009). IT-Governance an Universitäten - State of the Art und das Konzept der Universität Zürich. *Verwaltung & Management, 5*, 261-270.

Schwaiger, M. A., & Urbina, H. A. (2006). *IT Governance Frameworks for Compliance.* Royal Institute of Technology (KTH), Stockholm, Sweden.

Schwandt, T. (1994). Constructivist, interpretivist approaches to human inquiry. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 118-137). Thousand Oaks, CA, USA: Sage.

Sethibe, T., Campbell, J., & McDonald, C. (2007). *IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions.* Paper presented at the 18th Australasian Conference on Information Systems, Toowoomba, Australia.

Shaluf, I. M., Ahmadun, F., & Mustapha, S. (2003). A review of disaster and crisis. *Disaster Prevention and Management: An International Journal, 12*(1), 24 - 32.

Simonsson, M., & Hultgren, E. (2005). *Administrative Systems and Operation Support Systems – A Comparison of IT Governance Maturity.* Paper presented at the Proceedings of the CIGRÉ International Colloquium on Telecommunications and Informatics for the Power Industry, Cuernavaca, Mexico.

Simonsson, M., & Johnson, P. (2006). Defining IT Governance – A Consolidation of Literature. Royal Institute of Technology.

Simonsson, M., & Johnson, P. (2008). *The IT Organization Modeling and Assessment Tool: Correlating IT Governance Maturity with the Effect of IT.* Paper presented at the 41st Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, USA.

Smaczny, T. (2001). Is an alignment between business and Information Technology the appropriate paradigm to manage IT in today's organisations? *Management Decisions, 29*(10).

Software Engineering Institute, S. E. I. (2006). CMMI for Development Version 1.2. Retrieved December 11, 2007, from http://www.sei.cmu.edu/reports/06tr008.pdf

Software Engineering Institute, S. E. I. (2008). CMMI History. Retrieved June 29, 2008, from http://www.sei.cmu.edu/cmmi/faq/his-faq.html

Stake, R. E. (1995). *The art of case study research*: SAGE Publishing.

Strahringer, S. (1996). *Metamodellierung als Instrument des Methodenvergleichs: Eine Evaluierung am Beispiel objektorientierter Analysemethoden*. Aachen: Shaker.

Symons, C., Orlov, L. M., & Sessions, L. (2006). Measuring The Business Value Of IT. Retrieved March 19, 2007, from http://www.forrester.com/rb/Research/measuring_business_value_of_it/q/id/40267/t/2

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). Thousand Oaks, CA, USA: Sage Publications.

Taylor, S. (2000). *ITIL Series - Service Support, 15th Ed.* London, UK: CCTA Stationery Office.

Taylor, S., & Macfarlane, I. (2006). *ITIL V3 Small-Scale Implementation*. Norwich, UK: The Stationery Office.

Treacy, M., & Wiserna, F. (1996). *The Discipline of Market Leaders: Choose Your Customers, Narrow Your Focus, Dominate Your Market*. New York, NY, USA: Perseus Publishing.

Tsafarakis, S., Delias, P., & Matsatsinis, N. (2010). *Optimal product line design workflows using a service oriented architecture.* Paper presented at the 10th International Conference on Intelligent Systems Design and Applications (ISDA), Cairo, Egypt.

Tsubouchi, K., & Takata, S. (2007). Module-Based Model Change Planning for Improving Reusability in Consideration of Customer Satisfaction. In S. Takata & Y. Umeda (Eds.), *Advances in Life Cycle Engineering for Sustainable Manufacturing Businesses* (pp. 11-16): Springer London.

Turoff, M. (2002). Past and future emergency response information systems. *Communications of the ACM, 45*(4), 29-32.

Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The Design of a Dynamic Emergncy Response Management Information System (DERMIS). *Journal of Information Technology Theory and Application (JITTA), 5*(4), Article 3.

Turoff, M., Hiltz, S. R., White, C., Plotnick, L., Hendela, A., & Yao, X. (2009). The Past as the Future of Emergency Preparedness and Management. *International Journal of Information Systems for Crisis Response and Management, 1*(1), 12-28.

Ulrich, W. (2001). A Philosophical Staircase for Information Systems Definition, Design, and Development. *Journal of Information Technology Theory and Application, 3*(3), 55 - 84.

Van Bon, J., & Verheijen, T. (2006). *Frameworks for IT management*. Norwich, UK: Van Haren Publishing.

Van de Walle, B., & Turoff, M. (2008). Decision support for emergency situations. *Information Systems and E-Business Management, 6*(3), 295-316.

Van Den Eede, G., Muhren, W., Smals, R., & Van de Walle, B. A. (2006). *IS Capability for Incident Management and the DERMIS Design Premises.* Paper presented at the Proceedings of the 3nd International ISCRAM Conference, Newark, NJ, USA.

Van Den Eede, G., & Van de Walle, B. A. (2005). *Operational Risk in Incident Management: a crossfertilisation between ISCRAM and IT Governance.* Paper presented at the Proceedings of the 2nd International ISCRAM Conference, Brussels, Belgium.

Van Grembergen, W. (2002). *Introduction to Minitrack: IT governance and its mechanisms.* Paper presented at the Proceedings of the 35th Hawaii International Conference on System Sciences (HICCS), Hawaii, USA.

Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology : achieving strategic alignment and value*. New York: Springer.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2003). Structures, Processes and Relational Mechanisms for IT Governance. In W. Van Grembergen (Ed.), *Strategies for information technology governance* (pp. 1 - 36). Hershey, Pa.: Idea Group Publishing.

Venkatraman, N., Henderson, J. C., & Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal, 11*(2), 139-149.

Vogt, M., & Hales, K. (2010). *Strategic Alignment of ICT Projects with Community Values in Local Government.* Paper presented at the 43rd Hawaii International Conference on System Sciences (HICSS), Kauai, Hawaii, USA.

Vogt, M., Hales, K., Hertweck, D., & Finnie, G. (2010). *Strategic ICT Alignment in Emergency Management.* Paper presented at the Proceedings of the 7th International ISCRAM Conference, Seattle, USA.

Vogt, M., Hertweck, D., & Hales, K. (2011). *Strategic ICT Alignment in Uncertain Environments: An Empirical Study in Emergency Management Organizations.* Paper presented at the 44th Hawaii International Conference on System Sciences (HICSS), Kauai, HI, USA.

Vogt, M., Küller, P., Hertweck, D., & Hales, K. (2011). *Adapting IT Governance Frameworks using Domain Specific Requirements Methods: Examples from Small & Medium Enterprises and Emergency Management.* Paper presented at the Americas Conference on Information Systems (AMCIS), Detroit, MI, USA.

Walsham, G. (1993). *Interpreting Information Systems in Organizations*. Chichester, USA: Wiley.

Walsham, G. (1995a). The emergence of interpretivism in IS research. *Information Systems Research, 6*(4), 376-394.

Walsham, G. (1995b). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74-81.

Wang, W., & Belardo, S. (2005). *Strategic Integration: A Knowledge Management Approach to Crisis Management.* Paper presented at the Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Wang, W., & Belardo, S. (2009). The role of knowledge management in achieving effective crisis management: a case study. [Article]. *Journal of Information Science, 35*(6), 635-659.

Weill, P., & Broadbent, M. (1998). *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology*: Harvard Business School Press.

Weill, P., & Ross, J. (2004). *IT governance : how top performers manage IT decision rights for superior results*. Boston, Mass.: Harvard Business School Press.

Welch, J., & Welch, S. (2005). *Winning*. New York, USA: Harper Collins Publishers.

Weyns, K., & Höst, M. (2009). *Dependability of IT Systems in Municipal Emergency Management.* Paper presented at the Proceedings of the 6th International ISCRAM Conference, Gothenburg, Sweden.

Weyns, K., Höst, M., & Helgesson, Y. (2010). *A Maturity Model for IT Dependability in Emergency Management.* Paper presented at the Product-Focused Software Process Improvement, PROFES 2010, Limerick, Ireland.

Wilkie, F. G., McFall, D., & McCaffery, F. (2005). An evaluation of CMMI process areas for small- to medium-sized software development organisations. *Software Process: Improvement and Practice, 10*(2), 189-201.

Wilson, M. (2003). Rhetoric of Enrollment and Acts of Resistance: Information Technology as Text. In E. Wynn, E. Whitley, M. D. Myers & J. DeGross (Eds.), *Global and Organizational Discourse About Information Technology* (pp. 225 - 248). Dordercht, Netherlands: Kluwer Academic Publishers.

Wisner, B., & Adams, J. (2003). *Environmental health in emergencies and disasters*. Geneva: World Health Organization (WHO).

Wong, A. (2005). Theories used in IS Research: Hermeneutic Theory. Retrieved November 11, 2009, from http://www.istheory.yorku.ca/hermeneutics.htm

Yin, R. K. (2009). *Case study research: design and methods*. Thousand Oaks, CA, USA: Sage Publications.

Zave, P., & Jackson, M. (1997). Four dark corners of requirements engineering. *ACM Trans. Softw. Eng. Methodol., 6*(1), 1-30.